PERSEREC

AD-A281 541

COMPUTER CRIME: A PEOPLEWARE PROBLEM

PROCEEDINGS OF A CONFERENCE HELD OCTOBER 25-26, 1993

Editor: Theodore R. Sarbin

Defense Personnel Security Research Center
99 Pacific Street, Building 455-E
Monterey, CA 93940-2481

Defense Personnel Security Research Center

●99 Pacific Street, Building 455-E ● Monterey CA 93940-2481 ● 408 656-2448/dsn: 878-2448 ● Fax: 408 656-2041/dsn: 878-2041 email: 5210p@vm1.cc.nps.navy.mil

This report, *Computer Crime: A Peopleware Problem, Proceedings of a Conference Held October 25-26, 1993,* is a departure for PERSEREC and recognition that security has to come to grips with the expanding world of cyberspace. Many if not all the regulations that government writes to maintain the sanctity of information affecting the national interest assumes that information is that written on paper. We now know both the prospect and the problem that automation delivers: Individuals can dispatch information electronically, virtually without detection, given the right set of circumstances.

We conceived this conference to study the key element in automated information systems: the human *interface* with the computer. We design trusted systems with more than adequate safeguards for the protection of information. We install elaborate flagging devices to ensure that system integrity is not violated. Yet, we now realize that the human, or *Peopleware,* problem is the most vexing.

Much of the content of this report can be applied to any situation where insiders or determined outsiders gain access and do harm. Computers are the vector. They are the means by which a criminal end is reached. Nonetheless, the speed and stealth by which such information can be transmitted makes computer crime a dangerous threat to our national security. This group of security and computer professionals, both government and private, expresses concerns about computer crime that should be heard by a wider audience.

As with every PERSEREC report we ask that you contact us with your concerns and comments about the issue of computer crime. Either Dr. Sarbin or I would be pleased to discuss this paper or other work that might flow from it.

Sincerely,

Roger P. Denk, Ph.D.
Director

COMPUTER CRIME:
A PEOPLEWARE PROBLEM

PROCEEDINGS OF A CONFERENCE HELD OCTOBER 25-26, 1994

Editor: Theodore R. Sarbin

Defense Personnel Security Research Center
Monterey, California

TABLE OF CONTENTS

COMPUTER CRIME: A PEOPLEWARE PROBLEM

Summary

The Defense Personnel Security Research Center (PERSEREC) in Monterey, California, sponsored a conference in October, 1993, designed to increase understanding of computer crime and prepare the way for further research to improve personnel security measures. The title indicates the focus of the conference: Computer Crime: a Peopleware Problem.

The call for the conference was predicated on the recognition that despite the progress in the development of software and hardware countermeasures, break-ins continue to occur, and such break-ins are carried out by *people*. The objective of the conference was to share information and experience that would lead to research proposals the aim of which would be the creation of practices for controlling the criminal use of computers by both authorized users and unauthorized users (hackers). The latter class of criminal behavior has received a great deal of media attention, but the instances of fraud, sabotage, and espionage by employees with authorized access have received much less publicity.

To maximize interaction, we limited the number of conference participants to 15, augmented by members of the professional staff of PERSEREC. All participated, either delivering a prepared address or serving as a designated discussant. Ten papers were delivered over a two-day period. (Three of the speakers, Gail Thackeray, Michael Higgins, and Joshua Silverman, elected not to submit papers to be included in the Proceedings). The papers and the discussions provided information for outlining the parameters of information security, focusing on the fact of the vulnerability of more and more of the nation's secrets and also the trade secrets of American industrial companies that are stored in and transmitted through computer networks.

The extensive nature of computer crime and its control can be deduced from the varied professional orientations and interests of the participants. Taking part in the conference were government officials, computer security officers in industry, educators, criminologists, prosecutors, investigators, and psychologists.

Maynard Anderson, Acting Deputy Undersecretary of Defense for Security Policy, delivered the leadoff address. From his perspective--derived from more than three decades of work in intelligence, counterintelligence and security--he offered the observation, among other things, that good security practices and good management practices go together. In organizations where management and employee relations are deficient, the conditions are ripe for criminal acts. He referred to the observation made by a number of writers that loyalty to one's employer, one's community, even one's country, is no longer a primary virtue. We should all be concerned with the question: how to inculcate loyalty? He also suggested that security professionals examine their security awareness and deterrence programs from a moral rules perspective. Employees have acquired the moral rule, for example, about the importance of protecting tangible items of value in a vault. If an employee were to see an open vault, unmonitored, he or she would likely alert an appropriate officer. The same

employee might ignore a fellow employee copying sensitive files. In this example, the rule about protecting tangible property had not been extended to protecting intangible items in the form of data stored in a computer.

Dr. Sanford Sherizen is president of Data Security Systems, Inc. A computer security specialist with a background in criminology and sociology, he presented an analysis of the concept of deterrence and how the concept could be applied to information security. The concept of deterrence has been addressed in the sociological literature in connection with controlling more traditional crimes, however, it has heretofore not been systematically considered by computer crime experts. Some criminological theories on deterrence account for a potential criminal's resistance to an inviting criminal act as influenced by the knowledge that swift and stern legally-imposed punishment will follow with certainty. Other theories suggest that ties to family, peers, and workplace relationships are instrumental in controlling anti-social conduct. The development of appropriate deterrence policies and practices is hampered without knowledge of the extent and kinds of criminal activities involving computers. Such knowledge is meager, given the propensity of companies for not reporting criminal acts. Dr. Sherizen proposed mandatory reporting as a way of accumulating data on the nature and extent of computer crime.

Rhonda MacLean, Senior Manager, Computer and Communications Security for the Boeing Company, provided a case history of a break-in by two hackers. She identified the complicated technical, investigatory, legal and public relations problems that arose in dealing with the computer break-in. The apprehension and prosecution of the vandals required intensive cooperation between computer security personnel and management, and between management and law enforcement personnel. She brought out a point that was echoed many times: that computer crimes occur with unknown frequency because companies are reluctant to report the unlawful use of computers, either by authorized employees or by vandals. The reluctance is based upon the perception that public knowledge of break-ins would be an embarrassment and might result in customers' loss of confidence in the management of the company. She also showed a 12-minute videotape designed to educate employees in the essentials of computer security.

James P. Chandler, Professor of Law at George Washington University and Director of the National Intellectual Property Law Institute, provided a jurisprudential focus for the conference. He made a convincing case that intellectual property deserves the same legal protection as real property. Toward this end, he provided the conference with an in-depth look at the inadequacy of existing statutes and the need for legislative action to protect intellectual property stored in computers. In a world competing for industrial and commercial markets, the loss of intellectual property unprotected by existing law could be disastrous. An inherent threat to U. S. economic interests must be recognized in the absence of a global concept of intellectual property.

Gail Thackeray, Deputy County Attorney, Organized Crime and Racketeering Bureau, Maricopa County, Arizona, provided a lively discourse on the prosecution of computer

criminals, mostly youthful hackers. From the vantage point of 20 years experience as a prosecutor, she directed attention to the multifarious roles of the prosecutor dealing with youthful offenders. In a context in which the laws are sometimes ambiguous, and criminal intent difficult to establish, she brought into sharp focus the need for more precisely drawn statutes and for punishments appropriate to the crime. She suggested that hacking might be reduced if families were educated into the morality and legality of computer use. Some reduction in the frequency of hacking might follow from educational and public relations efforts to counter the belief that "computers are different," and the parallel belief that penetrations of computer systems are protected by the First Amendment. She offered some remarks about the effect of labeling youthful perpetrators as "hackers." Among certain segments of the youth culture, "hacker" has taken on heroic qualities; being identified as a hacker becomes a source of pride. The appropriate counter measure would be to encourage law enforcement personnel, prosecutors, and the media to employ pejorative labels such as vandal or thief rather than adolescent prankster or potential genius.

Joshua H. Silverman is a Trial Attorney in the Department of Justice, Criminal Division, Computer Crime Unit. He presented his views from the vantage point of a Federal Prosecutor. He identified three types of people who create the computer crime problem: (1) good people who practice bad security, (2) uninformed or misguided juveniles who intend no damage, and (3) bad people who engage in deliberate theft or vandalism. He recommended three approaches coordinate with the three types: education and awareness campaigns for users and corporations; education of juveniles, especially in the schools; and criminal law enforcement. To enlarge on the last-named approach, he summarized the federal statutes relevant to computer crime. Like Professor Chandler, he pointed to the limitations of existing legislation, for example, it is not illegal to write a virus.

Lynn F. Fischer, Technical Publications Editor, Department of Defense Security Institute, delivered an address that was billed as a challenge to security educators. He underscored the theme of the conference when he remarked, "information security in any type of environment is essentially a human issue...We can spend millions on NSA `trusted systems' but if the people who have access to those systems are not appropriately trained and are not trustworthy, it's all for nothing." He identified four propositions that should guide the security educator : (1) Information systems security and computer security in principle are not different from information security as traditionally practiced. The main point is that computer users need to be educated to regard computer security as a human issue in a technological environment. (2) Recent history demonstrates that no organization is immune from break-ins that result in significant damage by internal or external offenders. (3) We must be alert to threats from clever but misguided computer enthusiasts as well as foreign intelligence services. (4) Computer security managers and educators are not helpless in the face of potential threats. A number of proven practices are available to make employees aware of the threats and what to do about them.

Michael R. Higgins is the Deputy Director, Information Security Countermeasures Directorate in the Defense Information Systems Agency. He introduced his address with a

banner: Technology + People - Security. He emphasized an important observation regarding the technology-user interaction. As software and hardware technologists make their products more user friendly, security becomes more difficult. Further, diagnostic tools to discover inappropriate or unlawful use are always one step behind the technological advances. Under the heading "People are the problem," he identified the different perspectives of the principal actors in information system security. Users want only to access applications to get the work done. Systems administrators are interested in keeping the system up and available. Security managers focus on the command: protect information! These different perspectives have the potential for people to act at cross purposes. He offered some specific examples of the "people problem." One user gave a password to an anonymous system operator over the telephone. Another user ignored a malicious code for four months. A system administrator allowed a hacker to have an account to prevent trouble. Another system administrator failed to investigate system accounting discrepancies. Mr. Higgins closed his remarks with a description of the work of the Automated Systems Security Incident Support Team (ASSIST), a 24 hour help service for information security incidents worldwide.

LtCol Neil S. Hibler, Project Leader, Community Research Center, brought to bear a clinical psychological orientation. His group has been actively engaged in an effort to identify the psychological characteristics of citizen spies. Some of the more recently incarcerated spies made use of computers to gather sensitive and classified data for delivery to agents of a foreign power. The preliminary data on a small number of cases suggests that computer-assisted spies are not different from spies who trafficked in paper documents or microfilms. He presented a three-dimensional model for understanding the degree of risk for engaging in criminal behavior (computer-assisted or otherwise). In this model, risk is a function of (1) character traits (e. g., narcissism), (2) degree of dissatisfaction with life course (e. g., boring job), and (3) behavior options. The third dimension can vary from legitimate problem-solving action to risky behavior, such as substance abuse, absenteeism, suicide, sabotage, and espionage. The paper prepared jointly by Col Hibler and his associate, Jim Christy, presented detailed case histories, a significant feature of which was the inclusion of probes and questions for investigators relevant to assessing character traits, satisfaction with life course, and behavior options.

Dr. Theodore R. Sarbin, Senior Research Psychologist, PERSEREC, closed the meeting with a paper devoted to identifying some of the contextual conditions that lead an employee to engage in fraud, espionage, or sabotage. With the downsizing in the government and in many corporations, some employees will interpret the lay-off as an assault on their identities, a condition that fosters resentment. Some will act out the resentment through acts of sabotage. Employees with access to computer networks are in a position to sabotage information. In his presentation, Dr. Sarbin offered some concrete suggestions for managers to minimize the probability of a resentful employee engaging in unlawful or anti-social behavior to restore his or her identity.

Designated discussants for the papers were Richard H. Blay, Director of Security and Fire Protection, The Boeing Company; William S. Eyres, Director of Security (Western

Region) IBM; George P. (Pete) Grau, Chief, Security Countermeasures Center, CIA; Delmar M. Kerr, Instructor in Information Systems Security, Department of Defense Security Institute; Jack L. Torok, Information Security Division, CIA; Dr. Howard Timm, Research Psychologist, PERSEREC; Dr. Kent Crawford, Research Psychologist, PERSEREC; and Dr. James Reidel, Research Psychologist, PERSEREC.

Some afterthoughts: The papers and discussions brought out a number of interesting points. With the exception of the Hibler-Christy paper, very little attention was given to case studies of computer criminals. Their case studies produced some valuable tips for investigators and possibly for prosecutors. Gail Thackeray's lively account did provide us with a theoretical structure for understanding computer criminals, particularly hackers. She applied the familiar bell-shaped curve to socialization: at one end of the curve are the well-socialized individuals who would violate no legal or moral rules; in the middle are most of the population who might violate some rules under some conditions, such as, low risk or remoteness of possible punishment. At the other end are those individuals whom she identifies as sociopaths, Neil Hibler identifies as psychopaths, and Ted Sarbin identifies as undersocialized. To prevent such persons from accessing computer networks, we have to rely on software technology, and where the technology fails, to discover the offenders and, where possible, to prosecute. It would be an interesting exercise to study intensively the relationship of these undersocialized individuals to the computer. Some accounts suggest an addictive quality, as if the person has surrendered his or her self-control to the computer.

The people in the midrange of the construct require our attention. Most of our employees are in this mid-range. We do have psychometric instruments that would identify those people with a predisposition to violate the rules, to betray the trust. (PERSEREC has a nation-wide study in progress designed to validate a psychological test that would identify potential trust violators, a test that has already demonstrated its usefulness in screening for anti-social behavior.)

A few words are in order about the remarks made by Professor Chandler, Mr. Silverman and Ms. Thackeray, all concerned with the law, Chandler with creating laws and Silverman and Thackeray with applying them in a prosecutorial setting. In spite of what appears to be a wave of lawlessness, people do obey the laws. Empirical studies have shown a modest correlation between extent of knowledge of the rules and compliance with the rules. Chandler expressed so eloquently the complexities of creating laws to protect information. And the difficulties in applying the statutes is clearly no simple matter, as the prosecutors informed us. Yet, as Dr. Sherizen remarked, we have no where else to turn but to the law in order to provide at least a modicum of deterrence.

The excursion into the law helps us understand some of the problems faced by the security managers in the Boeing case history. At one point, it required the intervention of the courts to help locate the perpetrators of the criminal acts. The prosecutorial decision to accept a plea bargain was problematic: if the offenders had been convicted of a felony rather than a misdemeanor, they might have been deterred from engaging in further criminal acts.

A number of participants, notably Maynard Anderson and Lynn Fischer, observed that computer crime exists in a milieu of conflicting social forces. There are conflicts centered on free access to information (open vs restricted) and on the visibility of security measures (should computer security measures be obtrusive or unobtrusive, apparent or transparent?) In general, computer users want open access so they can get on with their tasks without having to deal with security hurdles. However, sensitive or secret information can be of value to people outside the organization--an argument for restricted access. This conflict leads to considering problems of insider versus outsider threat, and also whether to publicize security failures. If publicized too broadly, some users may be tempted to engage in criminal acts; if concealed or ignored, an insider threat may continue unabated.

Several participants stated the need for "threat examples" that could be used in persuasive communications to convince users and managers of the seriousness of the computer crime problem. It was suggested that intelligence agencies could reveal more information about computer crime cases (without damaging intelligence efforts) that would serve as "threat examples."

The array of experiences reported during the conference prompted the question: What would be the features of a model computer crime program? What would be the criteria for a State or Federal prosecutor to take action? A similar question is pertinent: What would be the features of a model deterrence and security awareness program? Answers to these questions are not simple nor inconsequential, an observation that directs security research professionals to formulate plans for systematic research.

Although it was the intent of the organizers of the conference to focus on insider crime as well as crimes committed by hackers, the latter received more attention. This differential distribution of attention may be the result of the practice of corporations to suppress reports of insider-generated crimes, as noted before. It is generally accepted that damage perpetrated by insiders such as occasioned by the theft of trade secrets, espionage, and sabotage is greater than that committed by hackers by a factor of at least 100.

During several of the discussions, the point was made that lack of cooperation among government agencies was sometimes responsible for difficulties experienced in investigating and prosecuting computer criminal activities. Resistance of law enforcement and prosecutors to following up leads provided by corporate system managers was also noted. It follows that effectively to prevent computer crime, steps must be taken to ensure cooperation among all parties involved.

Some of the participants remarked that existing legislation appears to be directed to the protection of information stored in government computers. Legislators need to be educated into the need for laws that would help corporate security managers to identify and to prosecute offenders.

Theodore R. Sarbin, Conference Organizer

Reasons, Rationale, and Responsibility in Computer Security

Maynard C. Anderson
Acting Deputy Under Secretary of Defense (Security Policy)

A forum concerning computer crime and computer sabotage would be expected to conclude with reasons why people use computers to commit crimes, and offer some ideas as to what might be done about it.

To begin with, Sarbin's definition should pertain--computer crime is the use of computers for espionage, sabotage, fraud, piracy, vandalism, etc., by persons who have legitimate access to computer networks.[1]

Historically, crime seems to follow accomplishment just as technological advances in military systems inspire the development of countermeasures. For example, the use of aircraft in war caused the creation of antiaircraft systems; intelligence collection activities spawn counterintelligence; radar absorbing materials that allowed the creation of low observable (stealth) aircraft were developed to defeat enemy systems of radar.

Accordingly, computer crime may well be the result of the development of automated information systems technology in combination with the changing attitudes of organizations which use the technology, and changes in the social behavior and moral values of the individuals who have custody of the machinery and their contents. Persons with access to computers become criminals when they exploit the weaknesses of an organization (and its leadership) for any number of reasons: personal gain, revenge, prestige among peers, to prove their superiority through satisfaction of ego driven desires (man over machine), or because they disregard the responsibilities of their stewardship and don't believe anyone else cares.

The computer is both a target, when it is a repository of information that can be converted into money, power, or some other advantage, and the means of its own exploitation when it serves as an extension of an intelligent operator's capabilities. The computer may become the compliant partner of the trusted operator in illicit as well as legitimate activity. The law of unintended consequences can be applied when advancements in technology make it possible to quickly, silently, and surreptitiously commit crimes that are most difficult to prevent and detect.

McCumber (1991) is quite correct when he concludes that most of the problems can be traced to interfaces and the most significant interface is the one between the human and the machine. He also reminds us of one of our own major failings--our ability to create eclipses our ability to control.[2] Sherizen echoes the same lament in agreement with McCumber that information security continues to fall behind technological advances.[3]

Sherizen also concludes that the field of information security tends to have limited understanding of the basics of criminal behavior, the use of personnel security approaches, and non-technical crime control measures.[4] Reasons for that might include the failure of management to integrate security techniques into operations, and a failure to understand the concept that security problems are seldom susceptible to treatment by a unique method. And, technical solutions are easier to use and understand because they are tangible. Abstract answers are not easily understood or accepted, but are easily overlooked or dismissed.

Sarbin discusses criminal activity and counter criminal activity as they relate to technological controls in the banking world.[5] A bank vault and a computer are somewhat different, however, in that the vault does not cooperate on command to defeat its own purpose. It is rather more inanimate in its steadfast purpose to remain unbroken. It is, in fact, a dormant, technologically moral device solely dedicated to protection. On the other hand, a computer is technologically amoral and does submit to the seductive manipulation of anyone able to apply proper directions. Security to the computer is merely an aspect of its operational life dependent on the abilities of its overseer.

Computer use today might be analogous to pre-Civil War slavery when the slave recognized the tenuous position of the overseer and used it to advantage. The overseer became dependent not just on the master, but also on the slaves to accomplish the mission. Computer security is designed to prevent crime and its application by an overseer is dependent both on the master of the computer, the organizational proprietor, and the employee operators. The conclusion that computer crime is not a technical problem but a human problem is reinforced. As McCumber reminded us concerning interfaces. we rely heavily on human review and intervention and are forced to make certain assumptions about human behavior.[6]

Over the years, experience has indicated that in organizations where good administration and management exist, there is usually cooperation among the leaders, overseers, and employees, in making things happen, and there will generally be good security. Where administration and management are deficient, so is security.

When management and employee relations are poor, the rationale for criminal acts sometimes involve blaming or scapegoating institutions. Personalizing the institution or the organization might help conceal a motive. Ensuring investment by the employee in the organization's mission might be a crime prevention measure. A basic premise in management remains that failure to have support of your constituency greatly diminishes your chance for success. Ensuring that everyone who has access to a computer has a stake in the reasons for the computer's integrity should improve the chances that those accessed will act in the best interests of their organization.

The computer and its software can be an aid to peopleware if there can be inserted into the daily operating schedules periodic reminders of the importance of the employee's position; a daily brief about progress of the organization and the employee's part in it; a daily motivational task for completion that will benefit the employees and strengthen their allegiance to the organizational objectives.

Such a technique is a combination of awareness and deterrence which creates a security environment for the employee that is conducive to proper behavior. Sherizen writes at some length about awareness and deterrence in his earlier PERSEREC report and in the paper prepared for this conference.[7] He refers to deterrence as an essential element in the control of criminal behaviors as it, theoretically at least, will frighten actual and potential offenders away from illegal acts. However, many individual as well as organizational factors intervene between the threat of legal sanctions and behavioral outcomes. Indications are that deterrence should be considered as a central concern in addition to the existing technical and managerial approaches to the prevention of computer crime.[8]

Everyone seems to agree that the computer criminal is an authorized user. Many of them are younger, and have some mechanical inclination. However, those that engage in fraud, embezzlement, insider trading, illicit business intelligence gathering, or obtaining advance information for bidding on Government contracts, may belong to an order cohort.

Sherizen writes that computer crime often involves non-traditional criminals.[9] That is arguable. Doesn't computer crime involve the commission of criminal acts using what once were non-traditional means? There may be situations, in fact, where criminal acts take place only because computers make them possible. Such circumstances might arise from a combination of the "subject" and "instrument" roles defined by the 1988 National Institute of Justice report cited by Sherizen.[10]

Some computer crime may occur because the computer allows the criminal to act remotely. As a silent crime, computer crime allows the act to take place apart from the results. The results are not manifest in the criminal's smell of gunpowder or sight of blood. The criminal doesn't have to crack a safe, carry money bags down the street on the run, or fence a valuable piece of jewelry; nor provide documents to a foreign government in a dead drop used for purposes of espionage. It must be easier for the criminal to rationalize the crime when the harm done is not sensorily perceived. Perhaps creating sensory perception of the crime would serve as a deterrent to some potential criminals.

Ensuring that people understand the reasonable use of hardware and software controls is really part of peopleware. If employees were allowed to show their interest by helping improve the use of security controls, by participating in the process, by improving the environment in which they function, their organization might even be able to diminish the resources used for hardware and software controls. Astute use of peopleware will improve the

quality of the work force. Employees might even identify the viruses and bugs among their peers and purge them.

The instrument, the criminal, the environment, and their interface are all factors of computer crime that are in a state of constant change. The core element is probably the criminal, or the potential criminal, and the ability of authorities to predict with any kind of certainty if or when the criminal will act.

When discussing forecasting in a time of great change, Rand's Carl Builder is of the opinion that human nature is not changing, but proliferations of people and technologies as well as evolution of ideas in the American society are changing predictably.[11]

"Predictably" is Builder's word, not mine. There are changes taking place that we might not wish to characterize as predictable. If they were predictable, probably we should have done something about them because some of the societal changes are undesirable.

Some of the changes will have an impact on the organizations and people of concern to us, not only in terms of the crimes that offend society but those that would have international consequences as a result of data manipulation to create false impressions, fabricate threat data, or issue bogus orders to units of the Government's-military services, all through the use of computers. An examination of the consequences of changes in the context of existing or potential opportunities for computer crime is required.

There is evidence that social controls and moral standards have weakened. James Q. Wilson asks, how can there be a moral sense if everywhere we find cruelty and combat, sometimes on a monstrous scale? One rather paradoxical answer is that man's attacks against his fellow man reveal his moral sense because they express his social nature. What is remarkable--indeed, what constitutes the most astonishing thing about the moral development of humanity--has been the slow, uneven, but more or less steady expansion of the idea that the moral sense ought to govern a wide range--perhaps, indeed, the whole range--of human interactions.[12]

That governance should include, of course, the interactions that are facilitated, stimulated and implemented by automated information systems as artificial, albeit most effective, influences on the abilities of people to perpetrate or enhance criminal activities with probably less likelihood of detection. The anomaly is that with the growth of the global economy and multinational corporations, often linked by computer networks, there are increasing opportunities for exerting a proper moral influence as well as for criminal activities of greater proportion and more far reaching consequences.

This aspect of the problem can be discussed in an institutional vein or a personal one. One of Wilson's comments applies:

"We want our actions to be seen by others--and by ourselves--as arising out of appropriate motives. And we judge the actions of others even when those actions have no effect on us."[13] His words are a reminder of comments attributed to the President of Mexico in 1913, when he allegedly said that we judge other nations by their actions, ourselves by our intentions.

Another possible reason for computer crime might be that loyalty doesn't seem to be in style these days. Professor George P. Fletcher, Columbia University Law School professor, simply states that loyalty is out of fashion these days in the marketplace as well as in peoples' personal, social and political lives. Fletcher attributes this to the fact that the world is too complicated for people--even philosophers--to figure out what is best for humanity at large.[14] That will never stop us from trying to figure out what to do to prevent, or dissuade, our personnel who are in positions of responsibility from acting irresponsibly.

Business ethics seem to have changed. Unethical practices in business are due to the great lack of civility in America according to Dr. M. Scott Peck.[15] His theory is that civility is all-embracing--a general awareness by people that personal well-being cannot be separated from the well-being of the groups to which we belong, our families, our businesses, our nation. That means loyalty to family, employer and country.

During the spring of 1992, the School of Business at West Georgia College, in an effort to determine human resource needs of its customers, conducted a survey to identify the skills, abilities, traits, and knowledges considered crucial to graduates' success in seeking employment and, thereafter, advancing to higher levels of responsibility within an organization. Among others, respondents were asked to identify what abilities and traits were crucial to their success in gaining employment and seeking job advancement. Acting in an ethical manner and loyalty to your employer were two of the traits ranked. The highest ranking was shared by three categories: make decisions, organize, and plan. The ability to make decisions and the ability to organize were considered the top two abilities by all groups, with the exception of business leaders ranking these skills as "3" and "2" respectively, and identifying the ability to act ethically as most important. The business leaders were from the northwest Georgia area while the survey in general was conducted among a sample of BBA and MBA Alumni who graduated from West Georgia College since 1973.[16]

Peck's theories and the West Georgia College survey demonstrate that business ethics might have changed, but the questions are how much and where, perhaps. If at least some business leaders consider the ability to act ethically important, that should mean that the environment they create for employees is one that would stimulate a lower incidence of crime. Perhaps influencing colleges and universities to emphasize ethics in their curricula would be a security technique which might reduce computer crime.

In attempting to determine ways in which security can be improved, examination of current systems by security professionals and outsiders as well, tend to focus on the process of security regardless of the context in which security techniques must be applied. It is not difficult to reach the conclusion that examinations of reasons for failure of security often overlook the proximate causes that created the problem in the first place. There might be contributory negligence on the part of the employer in a business circumstance when protection of the process through personnel security, information security, or even physical security, is disregarded in favor of enhanced production. Protection vs. profit is no doubt a significant conflict in many business and government environments today. Proper application of security techniques might actually enhance protection and profits. For example, if an organization attempts to protect all of the information involved in its activities, regardless of the information's sensitivity, the resource burden becomes overwhelming and real protection does not result because the custodians become immune to true sensitivity. "If everything is classified, nothing is classified." as the saying goes. Choosing proper security techniques and applying them with discrimination that is understood by the employees will result in better security and more efficient operations.

This leads to a conclusion that the security archetype, to use a Jungian concept, has not been properly developed over time. There probably isn't one yet for computer security because archetypes emerge from patterns. Our basic security archetypes which have, no doubt, caused our security professional's view of the world, need to be influenced and broadened to include everyone in any organization who has responsibility for maintaining the integrity of the organization's operations. Identifying the problem and trying to apply the best solution means that we must better manage the conditions that exist.

The focus of security has often been on safeguarding rather than prevention, probably at large and unnecessary cost. For every dollar spent on prevention, how much would be saved in losses as well as in safeguarding costs? There must be management anticipation of security issues that might be encountered. Reasonable expectations and judgement as to the application of prevention and countermeasures techniques will improve our abilities to deal with computer crime.

Mary C. Lawton, counsel for Intelligence Policy, Department of Justice, offered comments to the May 1993 Department of Defense Security Conference in Williamsburg, Virginia, under the title, "It's built, they came, but can they play?" She talked about having to play our game well and be adaptable enough to counter our proponents. She raised a broadly applicable legal issue in the context of the hacker: "We must take every possible measure to secure our databases against unauthorized access by hackers, but we are forbidden to monitor what the hacker accesses specifically, lest we invade his privacy." Another important message from Mary Lawton was one of cooperation among everyone concerned and focus of the efforts because computer security is part of a larger, more complex problem of managing information on a global scale today. The destruction or manipulation of data in information

systems may well be one of the most possible acts with the least likelihood of detection that has the greatest potential consequences for any organization on a universal scale. A challenge of this conference is to find more reliable means to determine and understand the forces and motives that cause all kinds of people to act irresponsibly and in disregard of the consequences of their acts.

Elements to consider in finding those means include:

- Determining the proximate cause of the opportunities for computer crime and the criminal's actions.
- Finding ways to restore ethical behavior to a place of high priority through education and training of leaders and work force.
- Making loyalty stylish.
- Developing a modern security archetype that places prevention in perspective with prosecution.
- Developing systems that relate the individual to his or her environment through involvement in administration and management of the organization.
- Maintaining employee awareness of correct behavior through use of hardware and software tools (awareness & deterrence).
- All the other things this conference will produce.

As a final note, Professor Chandler has been heard to say that "what we need is a concept of property which is not nationality dependent."[17] It would seem reasonable to say that we need a concept of security that is not category dependent but that includes every technique, every discipline, and every means to properly manage the control and distribution of things of value.

End Notes

1. Sarbin, Theodore R. "Computer Crime from a Criminological Perspective," Fourth Annual OPSEC Conference, May 12-13, 1993.

2. McCumber, John R. "Security measures for the State-of-the Art Workplace." *Security Awareness Bulletin*. Sept. 1991, pp. 5-9.

3. Sherizen, Sanford. "Computer Crime as a Unique Personnel Security Problem: " Understanding the Problem and Developing Potential Solutions, " Draft Report for the Defense Personnel Security Research Center, Monterey, California, August 1993.

4. Sherizen, Sanford. "Computer Crime as a Unique Personnel Security Problem. . ."

5. Sarbin, Theodore R. "Computer Crime from a Criminological Perspective."

6. McCumber, John R . "Security measures for the State-of-the Art Workplace."

7. Sherizen, Sanford. "Computer Crime as a Unique Personnel Security Problem. . ."

8. Sherizen, Sanford. "Can Computer Crime be Deterred?" Abstract for the Peopleware Conference, Monterey, California, October 25-26, 1993.

9. Sherizen, Sanford. "Computer Crime as a Unique Personnel Security Problem..."

10. Sherizen, Sanford. "Computer Crime as a Unique Personnel Security Problem..."

11. Builder, Carl H. "Is It a Transition or a Revolution?", FUTURES, March 1993, pp. 155-168.

12. Wilson, James Q. "The Universal Aspiration," The American Enterprise, The American Enterprise Institute, July/August 1993, pp. 31-39.

13. Wilson, James Q. "The Universal Aspiration."

14. Fletcher, George P. "What Ever Happened to Loyalty?", Bottom Line, August 15, 1993, pp. 13-14.

15. Peck, M. Scott. "All About Civility," Bottom Line, July 30, 1993, pp.1-2.

16. Gustafson, Leland V., Johnson, Jack E., and Hovey, David H., "Preparing Business Students--Can we Market Them Successfully?" Business Education Forum, April 1993, pp. 23-26.

17. Chandler, James P. "Intellectual Property and National Security," Fourth Annual OPSEC Conference, May 12-13, 1993.

Can Computer Crime Be Deterred?

Sanford Sherizen, Ph.D.
Data Security Systems, Inc.

Executive Summary

Deterrence is an essential element in the control of criminal behaviors. The primary objective of deterrence is to secure compliance with the law by detecting violations, discovering the perpetrators, and appropriately penalizing them to inhibit future violations.

Criminological theories on deterrence suggest that certain, swift, and stern legal punishments will control crime by frightening actual and potential offenders away from illegal acts. In addition, social scientists have suggested that informal "extra-legal" factors control anti-social behaviors through family, peer, and workplace relationships.

In this paper, deterrence is applied to information protection, based on the premise that deterrence should be considered as a central concern in addition to the existing technical and managerial approaches to computer crime prevention. There is a need for personnel security officials to determine how best to change the existing perceptions of employees and outsiders regarding the risks of getting caught in computer crime activities as well as the perceived payoffs from such activities.

Various concepts of deterrence are reviewed, followed by a discussion of what social science researchers know and don't know about the topic. Problems in applying the concept to computer crime are considered. The next section of the paper focuses on the particular types of computer crime and computer users appearing to have the most deterrence potential and the policy and program approaches needed in order to create deterrence within Governmental organizations. The discussion concludes with suggestions for a model research project that can specifically test deterrence as a computer crime prevention element.

1. What is Deterrence

Deterrence is an essential element in the control of criminal behaviors. Its primary objective is to secure compliance with the law by detecting illegal activities, discovering the perpetrators, and appropriately penalizing them in order to inhibit future violations.

Two forms of deterrence have been discussed by specialists. Special deterrence is the actual punishment applied to individuals who have committed a crime in an attempt to prevent them from committing additional crimes. General deterrence is the threat of punishment and applies to potential criminals who may consider committing crime and can be made to think about what has happened to those who were caught and punished.

Social thinkers have long been interested in achieving a "scientific" crime control which could lead individuals to decide against committing a crime. Evolving from the works of Becarria and Bentham, deterrence has served as an appealing concept for criminologists and legislators, offering a rational approach to limiting an individual's involvement or willingness to participate in illegal acts.

Deterrence practices have been built on the assumption that if the cost of an undesirable behavior can be increased, the behavior will decrease. Classical deterrence models posit that the effectiveness of the legal cost or threat is a function of how individuals perceive the certainty, severity, and celerity (swiftness) of punishment. Bentham stated:

> (T)he profit of the crime is the force which urges a man to delinquency; the pain of the punishment is the force employed to restrain him from it. If the first of these forces is the greater, the crime will be committed: if the second, the crime will not be committed (Quoted in Zimring and Hawkins, 1973, 75).

Stated as a formal model (Piliavin, et al, 1986), deterrence is:

$$E(U) = (1-p)\,U(y) + p\,U(y-F)$$

where E(U) = a person's expected utility from a contemplated activity

p= the likelihood of being punished for the activity

y= the anticipated returns (material or psychic) from the activity

F= the anticipated penalty resulting if the person is punished for the activity

This "rational-choice" behavioral model is based on the premise that humans are rational, hedonistic beings who know what is harmful to them, so that based upon a knowledge of laws and the fear of sanctions, they are able to choose and control their behaviors to avoid adverse consequences. Social control experts need only understand the correct "dosages" of rewards and punishments in order to lead individuals to behave properly.

Clearly, this mechanistic approach to human behavior and control structures is simplistic, both for its limited understanding of the complexities of rational behavior as well as its emphasis only upon formal legal sanctions. The varieties of human behaviors, the complexities of human perceptions affecting behaviors, and the often inadequate functions of social control make this approach problematic.

The "rational potential criminal" may apply to limited cases. People who contemplate committing a crime often have incorrect or unrealistic perceptions of the probabilities of being

sanctioned and of the severity of the sanction. Further, many people who commit crime act on impulse, either under the influence of drugs or alcohol or simply as the result of opportunity and need intersecting (Jacob, 1979).

As a result of these as well as other complications which will be examined, deterrence has been more discussed than proven as a functional social control option. Nevertheless, it continues to be considered as an important social policy.

2. What is Known About Deterrence

Comparatively little agreement exists in the research literature about deterrence and its application to criminal behavior (Piliavin, et al, 1986; Cook, 1980). In general, the little agreement that exists regarding deterrence is that the opportunity and reward components of the rational-choice model of crime appear to be operative under certain conditions while the risk or cost component, as measured by perceived risks of formal sanctions, does not appear to be operative (Piliavin, et al, 1986).

More specifically, the research can be summarized by three conclusions (Ibid, 102-103). First, research has failed to unearth a consistent deterrent influence of perceived severity of formal sanctions. Second, while most studies find a consistent but modest effect of perceived certainty of formal sanctions, others find that this effect is conditional, holding only for persons who are uncommitted to conventional morality. Third, the above results may be questionable because of methodological shortcomings of the studies from which they were generated.

Studies on drunk driving, as an example of a topic that has received research attention, suggest that severe penalties have limited, or at least inconsistent impact (Ross, McCleary and LaFree, 1990). Some evidence exists that punishment may have a quick but not a long-term deterrent effect. With publicity about mandatory confinement and other punishments developed to control drunk driving, arrests tend to increase. Ross (1982), however, concludes that over time, individuals learn that despite a crackdown, their chances of being caught are slim and, if caught, the chances of significant punishment are also slim. Thus, the deterrent effect is minimal.

There is also a growing consensus on the importance of informal social controls in deterring criminal behaviors. Extra-legal factors are informal sanctions that create compliance with socially accepted behaviors. In a review of trust violations (Parker and Wiskoff, 1991), the organizational literature reveals differing types of formal and informal controls over illegal behavior. Informal sanctions (co-worker reactions) can be even more effective than formal sanctions (corporate and criminal law) (Reichman, 1989; Hollinger and Clark, 1983). Conscience or internalized norms and attachments to significant others, including friends,

family, and colleagues/peers, can influence criminality by decreasing the expected gain or utility of crime (Sarbin, 1993). Shame and embarrassment are informal threats of sanctions that are important predictors for some individuals on whether they will become involved with criminal behaviors (Grasmick and Bursik, 1990).

In sum, various empirical social science studies on crimes lead to the conclusion that deterrence is much more complex than theory (and common sense) suggest. Criminals may not act as rationally as the theories assume, there are complicated rules affecting how an individual perceives risky situations, and many individual as well as organizational factors intervene between the threat of legal sanctions and behavioral outcomes.

3. What is Not Known About Deterrence

There are even more things about deterrence that are not known. The following quote is from a leading expert on deterrence and, though written many years ago, it summarizes the continuing lack of knowledge about this important concept.

> ...There are, however, a great many things about deterrence that we do not know. For instance, we cannot measure its overall effectiveness in the real world, and we are even less able to assign any share of the total effect to any particular mechanisms. Most practically, we do not know with any degree of precision how to weigh the variables which determine, in any particular case, whether deterrence will be effective. These include the personality of the individual to be deterred, his knowledge of the law, the situation he finds himself in, the rewards of the crime contemplated, the perceived likelihood of being caught and punished and the severity of the punishment (Zimring, 25).

Narrow research focus has contributed some to this limited knowledge of deterrence. Researchers have emphasized the external, formal legal control factors, such as the criminal law, which coerce, threaten, or sanction individuals. This has resulted in less appreciation of and and less research on the importance of the internal controls by which conventional norms are transmitted and learned by individuals as well as an overshadowing of the informal factors that play an important social control role. Whether deterrence is best produced by emphasizing internal, external formal or external informal controls continues to be a matter of controversy for social science researchers.

Relatively little is known about risk perception and behaviors as it applies to crime decisions, although there is a large literature on risk perception and decision making applied to other topics, including gambling and health (Sprent, 1988). Studies of risk perception and deterrence have failed to recognize the complexity of the perceptual processes that intervene between the threat or experience of legal sanctions and the behavioral outcomes. There is a

need to specifically examine computer criminal perceptions of punishment as well as risks (Cornish and Clarke, 1986).

Finally, it continues to be unclear from the research what strategies are most effective for increasing deterrence. There does tend to be agreement about the essential factors affecting an individual's decision to commit a crime. The most relevant include:

(1) crime control factors- the certainty, swiftness, and/or severity of punishments, both formal legal sanctions as well as interpersonal sanctions by family, friends, and significant others

(2) risk and profit factors-interactions of individual perceptions, objective cost-benefit realities, and behavioral activities

(3) individual ("internal") factors-how conventional norms are accepted by individuals as moral reasoning and self-image concerns

(4) crime opportunities- the protective safeguards in place, crime event decisionmaking, and the opportunity costs considerations

Yet, how much each of these contribute to the crime decision or how each of these can be changed in order to deter crime is not certain. At this time, there are no sure ways to know which social policies on deterrence are most effective or could be considered as an appropriate means to diminish crime.

As a result of the lack of knowledge about this critical concept, one leading researcher has concluded that the extensive deterrence research undertaken by social scientists "...so far has produced little more than a frame of reference, a variety of hypotheses and suppositions, and a scattering of empirical observations which are more anecdotal than systematic" (Cook, 1980, 212).

4. Why Deterrence Should Be Central to Computer Crime Prevention

It should be clear from the information presented that deterrence may be too unclear or complicated to be used effectively. Yet, despite this uneven and often contradictory picture of the effectiveness of deterrence, it is important to consider how to place it within computer crime prevention efforts. A deterrent perspective can help to guide national policy, particularly in making computer crime and related laws more effective in curbing computer crimes and abuses. Even limited success with deterrence can provide some protection from an increasing number of computer crimes and the growing seriousness of the problem.

In order to work, deterrence should be integrated with other computer crime control approaches, providing messages to actual as well as potential computer criminals that such crimes will be punished. Deterrence should be considered as a central concern in addition to the existing technical and managerial approaches to computer crime prevention.

At this time, deterrence is not considered as an important aspect of information security and computer crime prevention. This lack of consideration is less due to a feeling that deterrence cannot work than for operational reasons. While legislators and attorneys may consider the issue in their deliberations, information security personnel are more concerned with the direct issues of prevention and detection rather than the broader issues of determining an ideal punishment scheme. Organizational lawyers and senior executives make deterrence-related decisions but must weight reputation and other critical organizational concerns. If organizations choose not to press charges against an individual found committing a computer crime or abuse in order to protect the organization's reputation, that "letting someone get away with it," even when the person loses their job and is punished in other ways, sends a clear message to other employees. Thus, the current treatment of information protection problems may well run counter to deterrence.

There is a need for personnel security officials to determine how best to change the existing perceptions of employees and outsiders regarding the risks of getting caught in computer crime activities as well as the perceived payoffs from such activities. That will not be easy but there are several applied social science options available.

As with other white collar criminals, computer criminals are often more easily dissuaded that are "less rational" criminals who commit illegal acts when opportunities occur rather than as a result of planning their crimes. Further, the extra-legal social stigma and negative affects on job opportunities can be powerful incentives to prevent certain middle-class persons from becoming involved with computer crime. In these ways, certain forms of computer crime and certain potential computer criminals are more deterrable than others.

Making deterrence part of computer crime prevention will not be an easy effort. As difficult as deterrence is to apply, computer crime makes an even more difficult target. The variety of computer crime activities tends to complicate the determination of what would be the best deterrence policy choices. What might work for teenaged hobbyists might not work for destructive hackers. Average users might be more affected than technically skilled users. Individuals might be deterred but managers who decide to use computers for organizational gain might not be (Braithwaite and Makkai,1991). Deterrence might work in one industry but not work in another industry. Further, computer use now involves a variety of environments, including home, school, work, hobby, etc.. All of these have different controls (or lack of them) and an inconsistent and non-sequential ability to influence behaviors.

At a minimum, there are a number of legislative, law enforcement, and organizational changes that are required for deterrence to work effectively. These are covered in detail in the next section.

5. Applying Deterrence to Computer Crime Prevention

Partial answers about deterrence are possible, at least in terms of where deterrence emphases need to be placed. Legislative, law enforcement, and organizational changes need to be made in order for deterrence to be effective with computer crime.

Legislative Changes

Deterring computer crime will require the public sector to pass improved legislation (Charney) and the private sector to study, develop, and implement appropriate security measures. (Roache) Computer crime deterrence requires more apprehension and punishment in order to function (Sherizen, 1985). Even though there are 49 state computer crime laws and a number of Federal computer crime laws, there have only been a handful of criminal prosecutions (U.S. National Institute of Justice, 1991). If the perception of the certainty and severity of punishment is a key variable in explaining deterrence, then the law has not been an effective force in controlling computer crime (Nelson, 1991). Deterrence of computer crime should focus on tailoring penalties to computer crime severity, with special attention being paid to key information processes, industries, and types of violations. As important, there is a need to consider revising wire and mail fraud laws so that they more directly cover new technological development. These fraud laws, as well as other laws, have often been used by prosecutors in place of the weak and outdated state and federal computer crime laws.

Changes are also necessary in terms of mandatory reporting. One federal prosecutor (private conversation) suggested that computer crime will not be controlled until organizations are required to report these crimes to law enforcement. Such a requirement would maximize opportunities for the authorities to determine which cases require legal attention rather than to await cases depending upon the willingness of organizations to press charges. Interestingly, the Federal Sentencing Guidelines (Sherizen, 1993 B), which emphasizes the reporting of crime (as well as detection and prevention) and recent SEC barring of Salomon executives from further Wall Street activities due to their lack of reporting of underling's illegal acts may serve as a warning shot to managers. The suggestion of the Department of Justice to the U.S. Sentencing Commission that the federal computer crime law be considered for inclusion under the Guidelines could increase organizational attention to this issue even further.

Law Enforcement Changes

Legislation and regulation alone will not be sufficient, however. If deterrence is to become more of a computer crime prevention issue, law enforcement aspects of computer crime prevention, such as current resource limitations on investigation and prosecution of computer crimes, will also have to be addressed. In many ways, deterrence involves risk and "payoff" decisions by individuals (Katz, 1988). For most individuals who commit computer crimes, detection and punishment are so infrequent that this would seem to be of little concern to them. Those few computer crime cases which have made it into the criminal justice system have not led to speedy or severe punishments. At times, cases are mishandled by law enforcement agencies (Stoll, 1989), raising questions about the effectiveness of the law.

Organizational Changes

Beyond formal laws and regulations, there are other possibilities for applying deterrence to computer crime. One possibility is to focus on countering the social influences that lead people to commit crimes. Researchers have found that controls over certain illegal behaviors were associated with moral commitment (internalization of legal norms), fear of social disapproval, and fear of legal punishment (Grasmick and Green, 1980). Relating that to computer crime, it is clear that organizations can attempt to influence perceptions of appropriate computer behaviors.

To a large degree, employees are influenced in their views about "normal" computer use and computer crime as a result of group interactions. Individuals make decisions, including risk decisions, as group members and are influenced by group norms. In that sense, an individual's perception of risk can be modified by the tendency of a group discussion to shift the preferences of members of the group toward more risky choices than they would have selected as individuals (Myers and Lamm, 1976). On the other hand, if the group process can be influenced by deterrent messages, then this may be an effective means of swaying individual perceptions toward viewing increased risks of computer abuse activities.

Deterrence of computer crimes can take other behavioral forms. For some employees, minimizing their opportunities to legitimize or neutralize their crimes forces them to understand what are and what are not appropriate activities. Sykes and Matza (1970) suggest that there are five major types of neutralization. These are (1) denial of responsibility, (2) denial of injury, (3) denial of the victim, (4) condemnation of the condemners, and (5) appeal to higher loyalties. Relating this to computerized activities, an organization can attempt to specifically counter these attempts to redefine crimes, forcing employees to understand that there are no justifications for what they are attempting.

This countering of justifications is particularly important for two reasons. First, computerized environments remove people from direct access to many of their work

functions, with work "disappearing behind the screen" (Zuboff, 1990). Work consists of pushing keys, moving data files, and other abstract work that can remove the individual's feel of control and involvement as well as responsibility for his or her acts. Second, the downsizing of the Government and other economic threats that are striking the American labor force are causing anger and resentment among employees (Sarbin, 1992). The result is a situation that easily allows individuals to view themselves as victims and to structure their criminal activities as something that is appropriate, allowable, and, in a word, a "non-crime".

Organizations can minimize these "non-crime" viewpoints by developing:

(a) information security awareness training that directly stresses what is (a) crime, viewed legally as well as ethically

(b) social control mechanisms that stress group norms and social embarrassment which stress that such activities let down colleagues and co-workers (Reichman, 1989)

(c) deterrence for employees using computer systems by finding and questioning work errors, providing prompt security warnings, and highlighting the fact that there is control and security monitoring in place

(d) distribution of information about the punishments that have been given to convicted computer criminals

Finally, computer crime can be perceived by employees as a "normal" response to organizational structure. This crime can be controlled by changing the organizational climate and/or how it is perceived by employees. A "criminogenic" environment (Sherizen, 1993 A) is where the organizational culture, values, and structure unwittingly contribute to crime by sending certain messages about crime. Security managers should determine if their organization has such an environment and, if so, what can be done to change those messages. Surveys of how employees view information security and computer risks would determine whether an organization is producing positive or negative messages about crime. Do employees perceive that access control measures are put in place? Do they feel that security mechanisms are operating? Do they assume that their bosses have little interest in security? Are crimes often found in the organization, indicating organizational vulnerability? If these factors are found, the organization may have a climate that supports or in other ways fosters computer crime. If this is true, then security personnel need to actively change organizational structures and employee perceptions (Ibid, 1993).

It is clear that making deterrence a computer crime prevention option will be a difficult undertaking. There are, however, specific changes which are available that can lead employees and others to learn that computer crime does not pay.

6. Critical Research Needed on Deterrence & Computer Crime Prevention

Much more focused information is needed on the role of deterrence in preventing computer crime. It would be worthwhile for PERSEREC or some other Government entity to consider funding a sophisticated research and policy study of the problem.

A more extensive review of the literature than was possible for this paper should be made, leading to a synthesis of what is known about deterrence in its various forms and a "translation" specifically applied to computer crime control. Beyond the literature review and synthesis, there is a need to empirically determine how non-criminal ("average") computer users perceive and make their rational decisions about appropriate behaviors and how effectively rules as well as penalty threats are communicated to them. This could lead to comparative studies of computer criminals.

Similarly, a survey of known as well as "hidden" computer criminals to determine their risk perceptions could provide insights into methods to increase their perceptions of risk for computer crimes. Techniques are available in criminology to study the decision-making of computer criminals as it actually occurs in natural settings by asking subjects to specify how they made critical decisions (Clarke and Cornish, 1980).

Deterrence is too important to information protection to leave the concept in its present unfocused mode. A focused effort to clarify its meaning and to apply it to the computer crime problem can pay enormous dividends to public order.

Bibliography

Braithwaite, J., & Makkai, T. (1991). Testing an Expected Utility Model of Corporate Deterrence. *Law and Society Review, 25*,(1), 7-39.

Charney, S. (1992). *The Computer Crime Initiative: The Justice Department's Response to the Growing Threat Posed by Computer Criminals.* Washington, D.C.: Department of Justice.

Cook, P.J. (1980). Research in Criminal Deterrence: Laying the Groundwork for the Second Decade. In N. Morris & M. Tonry, (Eds.), *Crime and Justice: An Annual Review of Research*, Vol 2. Chicago: University of Chicago Press, 211-268.

Cornish, D.B., & Clarke, R. V. . (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending.* New York: Springer-Verlag.

Clarke, R.V., & Cornish, D.B. (1980). Modeling Offenders' Decisions: A Framework for Research and Policy. In N. Morris & M. Tonry, (Eds.), *Crime and Justice: An Annual Review of Research*, Vol. 2. Chicago: University of Chicago Press, 147-185.

Grasmick, H.G., & Green, D.E.. (1980, Fall). Legal Punishment, Social Disapproval and Internalization as Inhibitors of Illegal Behavior. *Journal of Criminal Law & Criminology*, 71, 325-335.

Hollinger, R. C., & Clark, J. P. (1983). *Theft by Employees.* Lexington, MA: Lexington Books.

Jacob, H. (1979). Rationality and Criminality. *Social Science Quarterly, 59*, 584-85.

Katz, J. (1988). *Seductions of Crime: Moral and Sensual Attractions in Doing Evil.* New York: Basic Books.

Myers, D. G., & Lamm, H. (1976). The Group Polarization Phenomenon. *Psychological Bulletin, 83*, 602-27

Nelson, B. (1991, April). Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm. *Computer/Law Journal, 11*(2), 299-321.

Parker, J. P., & Wiskoff, M. F. (1991). *Temperment Constructs Related to Betrayal of Trust.* Monterey, CA: PERSEREC.

Piliavin, Irving, et al. (1986). Crime, Deterrence and Choice. *American Sociological Review, 51*, 101-119.

Reichman, N. (1989). Breaking Confidences: Organizational Influences on Insider Trading. *The Sociological Quarterly, 30*, 185-204

Roache, J. Y. (1968). Computer Crime Deterrence. *American Journal of Criminal Law, 13*, 3 (Summer), 391-416.

Ross, H. L. (1982). *Deterring the Drinking Driver: Legal Policy and Social Control .* Lexington, MA: Lexington Books.

Ross, H.L., McCleary, R., & LaFree, G. (1990, Spring). Can Mandatory Jail Laws Deter Drunk Driving? The Arizona Case, *The Journal of Criminal Law & Criminology*, No. 1, pp. 156-159, 163-164.

Sarbin, T. R. (1993) *The Power of Resentment: Some Observations on Trust and Betrayal with Special Reference to Computer Crime*. A talk delivered at the Fifth Annual Conference of the Department of Defense Security Institute, Williamsburg, VA, May 4-8.

Sherizen, S. (1985). *Federal Computers and Telecommunications: Security and Reliability Considerations and Computer Crime Legislative Options. A Contractor Report for the Office of Technology Assessment*, February, 1985. (Available from NTIS as Report PB 86-208931.)

Sherizen, S. (1993 A). *Computer Crime As A Unique Personnel Security Problem: Understanding The Problem And Developing Potential Solutions*. A Report Prepared for PERSEREC, Monterey, CA.

Sherizen, S. (1993 B). *Federal Sentencing Guidelines: New Information Security Management Considerations*. (Unpublished) Natick, MA: Data Security Systems.

Sprent, P. (1988). *Taking Risks: The Science of Uncertainty*. New York: Penguin Books.

Stoll, Clifford. (1989). *The Cuckoo's Egg*. New York: Doubleday.

Sykes, G., & Matza, D. (1970). Techniques of Neutralization: A Theory of Delinquency. In M. E. Wolfgang. et al., (Ed.), *The Sociology of Crime and Delinquency*, 2nd ed. , New York: John Wiley, 292-299.

U.S. National Institute of Justice. (1991). State Computer Crime Statutes. Washington, D.C.: Government Printing Office.

Zimring, F. (1971). *Perspectives on Deterrence*. Public Health Service Publication, No. 2056, Chevy Chase, MD: National Institute for Mental Health.

Zimring, F., & Hawkins, G. J. (1973). Deterrence. Chicago: University of Chicago Press.

Zuboff, S. (1990). *In the Age of the Smart Machine: The Future of Work and Power*. New York: Basic Books.

The Boeing Hacker Incident

Rhonda E. MacLean, Senior Manager
Boeing Computing & Communications Security

BACKGROUND:

With the cold war behind us, we see an increasing focus on competitive advantage in a global market. This factor is currently influencing the way we do business and will continue to do so for the foreseeable future. Corporations are beginning to recognize the value of intellectual property and its overall contribution to maintaining a competitive edge. At the same time, corporations are using automated systems to further ensure their ability to compete in a world where business transactions are handled in micro seconds versus weeks or months.

Computers and telephones have progressed far beyond boxes on a desk, and are now gateways to business highways. Many corporations are harnessing the latest technology, enabling them unlimited access to world-wide communication networks of data, voice and video. The speed at which technology changes are faced today may pale when compared to the pace of change in the future. It is widely accepted that increased computer usage and computer controlled media will be the "norm" for business transactions.

Protecting those systems and the information contained on them is being reevaluated by many corporations today as a business priority. Unfortunately, a compromise of those systems is sometimes required to get the commitment necessary to ensure a level of appropriate protection is in place and sustained.

CASE STUDY:

The Boeing Company received a wake up call in October 1992 when one of it's major computer supplier's called and wanted to know why a Boeing userid was trying to gain unauthorized access to their systems. It was determined the userid in question belonged to a manager who had not used the account for several months. In reviewing the system logs, it was easy to confirm the userid was being used by someone who was not authorized.

By reviewing previous records, we were able to determine the unauthorized activity had been going on for at least a month before the call from the outside supplier. Because the intruders were using an "authorized" account which was not being actively used or monitored by the account owner, the unauthorized activity was not noticed. When the account owner subsequently received his monthly computing charges, he was surprised to see the amount of usage logged by the unauthorized users.

Further investigation revealed the intruders gained access [illegible]ung modem. Off-the-shelf software made possible rapid sequential dialing that [illegible]ed the process. Once the intruders reached a computer, in this case Boeing's computer, the rest was easy. The local area network password file was stolen yielding access to a number of other valid user accounts. Even though passwords are encrypted, password cracking software made easy work of revealing the necessary passwords.

Exacerbating the problem, the violated computer system had established "trusted" network connections with other computer system inside and outside The Boeing Company. Taking advantage of this "trust," the intruders were also able to gain unauthorized access to other commercial industry, government agency and educational systems. Those organizations were immediately notified and an agreement to work together with law enforcement was quickly established.

While briefing management and developing an internal strategy on the situation, the activities of the intruders were continuously monitored. The recommendation to allow the intruders to continue unauthorized access while working with law enforcement was approved with the provision that if any "malicious" activity was detected, we would immediately close the door.

Concurrently, a response team was formed comprised of computing security specialists, technology support persons and a computing security representative from each operating division. This team met daily to review current activity, status and to plan the next steps. This team, together with the response processes they developed, would later provide the basis for developing an internal computer emergency response team.

The company Computing & Communications Security organization took the lead in coordinating the internal activity as well as interfacing with law enforcement agencies. In addition, the company's legal representative was instrumental in assisting the group and in working with law enforcement. The size of the response team was kept to a minimum and each member was advised to maintain confidentiality. The objective was containment wh[illegible] minimizing the risk of "tipping our hands" to the intruders.

Senior managers were briefed daily as to intruder activity. Each day the decision to leave the access open or to begin closing the door was discussed. In addition, we briefed a senior public relations executive to deal with the news media once the activity became public. This proved to be an important element later in the case.

Although we initially contacted the Federal Bureau of Investigation (FBI), it was unclear which law enforcement agency would actually have authority. We felt confident that both state and federal computer trespass laws would apply. Therefore discussions were also held with city and county police departments having jurisdiction where the equipment was located.

Resolution as to jurisdiction came only after careful review of additional evidence and discussions with the law enforcement agencies on the range of laws being violated.

During review of the activity, Boeing investigators determined the intruders were using Boeing computing resources primarily to crack passwords. One very important password file moved to the Boeing system by the intruders in order to crack it, was found to belong to the United States District Court for the Western District of Washington located in Seattle, Washington. The intruders had successfully broken several passwords and gained access to the court's computer. It was this fact primarily that resulted in the FBI's jurisdiction (felony violation of Title 18, USC, Section 371, "Conspiracy to Defraud the United States Government").

The level of concern and the stakes were substantially raised once the intruders had shown interest in the federal court's computer. The information it contains is considered extremely sensitive and its compromise could have had very serious ramifications. If the intrusion had been confined to only one company's computing system, it is unclear if the case would have been considered serious enough for any prosecution to have taken place.

At this point there was still no clue as to who the intruders were or where they might be operating from. The FBI asked the U. S. District judge for a court order to allow the placement of a pen trap on the Boeing telephone line to obtain the telephone number being used to access Boeing's systems. This proved to be more difficult than anticipated and resulted in an important lesson learned.

The unforeseen problem came as a result of Boeing's logon message, presented any time a user is initializing access. The logon banner notified users that it is a private computing system restricted to authorized users only. Unauthorized users are advised to disconnect at once. Further, the banner notifies unauthorized individuals that actual or attempted use would result in criminal and civil prosecution. However, the banner failed to notify persons attempting access that the company reserved the right to review, monitor and record without notice or permission. Additionally, the logon banner did not say that information obtained by such monitoring, review or recording was subject to review by law enforcement in connection with the investigation or prosecution of possible criminal activity on the system. In spite of this deficiency the court allowed a trap to be placed. It is unknown if this would have proved damaging had the case gone to trial.

Nonetheless, those missing items in our logon banner cost several days delay in obtaining the court order. Creating further delay was the fact that the phone company was unable to accommodate the request for a trap in a timely manner due to lack of resources. They were working higher priority cases, and because ours did not involve personal endangerment we had to wait. After a week of waiting and applying pressure from all possible sources on the phone company, the trap was at last installed. Once it was in place, a telephone

number was obtained and traced through telephone company records to a dormitory phone at a local university. At the same time, a recording device was installed that recorded the hackers' activity. Other than password cracking, their other main interest centered on reading the e-mail of Boeing system users. At this point it didn't take long for the FBI through their investigative efforts to identify the two hackers.

By this time over two weeks had gone by and the decision was made to go ahead "quietly" with the recovery part of our plan. Although we wanted to begin closing our door, we knew this could tip them off. In order to, without a doubt, prove who's hands and faces were behind the computer, it was imperative to catch the intruders in the act. It was felt that even though the risk was low that every password had been cracked on Boeing's systems, we decided to take no chances. We starting distributing a number of security software tools to system administrators and asking them to reset all passwords on their systems. Consequently, our plan required us to ask system administrators to bring down production computer systems. This assured closing down the intruders' access. The administrators needed executive management's approval to bring down production systems for password resetting. To obtain this approval, we decided to have key executives in each division sign a letter authorizing our system administrators to follow designated instructions to bring down the systems. The letter also emphasized to administrators the extremely sensitive nature of the issue and were advised not to discuss it with anyone. Here we learned another hard lesson.

These memos turned out to be a strategic error. While they were hand delivered to only a very few people, it took less than an hour before someone in the company faxed the letter to a local radio and TV station. Before the close of business, it had hit the local news. By early evening, national news agencies had begun to pick up the story. We felt fortunate that we had previously briefed our public relations executives so they were prepared to handle the situation.

The premature disclosure that someone was "breaking into Boeing's computers," forced Boeing and law enforcement to change their plans immediately. Obviously our plan to synchronize the arrest with the FBI was compromised. Their agents were forced to switch quickly to plan "B." Arrests of the two hackers were made the following week, and a full confession was obtained. As is typical in these cases, the hackers were initially quite proud of what they had done and consequently were more than happy to show how smart they had been.

In many ways our intruders were typical of nondestructive hackers. Their motive was to "network navigate" (a "hacker" term used to describe a game whose objective is to see how many computers they could access and browse through). Both hackers had prior records for theft of computer equipment.

As a result of this case, they were arrested in November 1992 and charged with a felony violation of Title 18, USC, Section 371, "Conspiracy to Defraud the United States Government." In February 1993, the charges were plea bargained to a misdemeanor, violation of the "Computer Fraud and Abuse Act of 1986," Title 18, USC Section 1030 (a) (3) and Section 2, "Computer Trespass." In June 1993 the hackers were sentenced to 250 hours of community service, S years probation, and $30,000 restitution ($28,000 to Boeing). Since the closing of this case, both individuals have been re-arrested for violation of parole for the theft of credit card numbers and cellular phone fraud.

CONCLUSION:

Traditionally the potential loss of competitive information has been the objective in providing a level of "due care." However, the integrity and availability of the information is also a major consideration in abating risk. Hackers who "network navigate," or browse, are of concern not only because they are stealing company time on computers but because they may inadvertently compromise the "integrity" of the information. In some cases an unauthorized intruder can totally disable a computing or telephone system, consequently denying service for authorized users. This is not just a mere inconvenience. The real costs to the company are measured in terms of lost production and lost revenue.

As the technology and the automated business environment evolves, we see an alarming trend in which computer and communication system intrusions are the basis for criminal activities and/or monetary gain. There is a significant difference between the adolescent prankster and the criminal who has virtually unlimited access to corporate and government information.

This change has happened so rapidly that many managers and corporate executives are unaware of the threat. It is especially difficult to quantify the threat in tangible terms because current statistics are unreliable, and in many cases, unavailable.

At a recent conference of information technology security managers, the attendees were asked if their companies had been violated by hackers. Roughly one-third of the audience raised their hands. Secondly, about ten percent stated they had not, to their knowledge, been violated by hackers. Subsequently, the question was expanded to ask how many of their companies would not admit to whether or not they had been violated. The much larger portion of the group indicated an affirmative answer to this question, demonstrating further the reluctance of many companies to disclose this type of information.

Unfortunately, as demonstrated above, some company management will not admit their systems have been violated. They often fear they are exposing corporate vulnerabilities or their own negligence in failing to exercise "due care." In addition, the specter of civil liability

may prevent some corporations from notifying other victims who may be affected by the admitted remiss. Increasingly though, many companies are realizing that it is in their best interest to be conscientious and to view cooperative disclosure as being a "good business citizen."

The law in this area appears to have been set up primarily to protect government and government related industry, but not industry as a whole. Therefore this complicates the ability of private industry and legal authorities to adequately deal with these crimes. Tracking information technology crimes back to a human person in real-time is a challenge the legal community must address. A heightened technical competence is required to solve and present to lay jurors these technically complex cases in non-technical terms. With these challenges, industry and government must increase their training and support for improved security policy and tools.

Boeing began its computing security program back in the early 80s focusing on security for critical systems. During the last decade, increased emphasis has been placed on this program and now every computing system within Boeing is required to do an annual security self-assessment. This program has made great strides in the area of prevention and detection. But as we learned from this case, there are those whose determination can outwit the best of prevention and detection methods. Employee awareness is often viewed as one of the strategic defenses against such attacks. In 1992, Boeing's corporate computing board approved a plan requiring all users of company computers to attend an annual security awareness briefing. These briefings are designed to educate employees on the threat, what to look for, and their role in protecting our systems and information. The briefings also discuss the importance of information security to our company's long-term competitiveness. We see our awareness activity as the cornerstone to a good security program.

In conclusion, government and private industry must begin communicating openly about the threat and sharing their experiences. As a group, the synergy will only strengthen our ability to address these issues in the future and protect America's economy and technological advantage.

Computer Crime: Legal Aspects

James P. Chandler
Director, National Intellectual Property Law Institute

I. INTRODUCTION

Laws prescribing computer system violations have proceeded along two separate and distinct lines. First, copyright laws have been written that include protection of copyrights of computer software. Civil and criminal penalties are included to deter violations. Second, computer crime bills have been proposed that punish the unauthorized access of a computer system with resultant damage. Criminal penalties are provided for in the computer crime bills. As each of these lines progress, they come closer to intersection. A Federal computer crime bill, S. 1322, has been proposed that may be interpreted to incorporate state and Federal courts' view of software as property, the taking of which may rise to the of "damages" for purposes of S. 1322. Further, a new Federal copyright bill, S. 893, provides for criminal penalties for violations of a copyright.

This paper asserts that information in the form of software may now be deemed property, the theft of which rises to the level of damages under the proposed computer crime law. The copyright bill, as a parallel development, makes serious software copyright violations a felony. The allowance of software as property, and, the states' and the Federal judiciary's expanded definition of damage in the context of theft of information now links these two lines of legal development.

First, this paper will introduce the reader to issues encountered in computer crimes by presenting several examples of computer crime. Second, selected state and Federal legislative and judicial responses to these computer crimes will be discussed. Third, the crucial changes in the common law and the statutory definition of property as a response to computer crime will be detailed. Fourth, the notion of information as property in a Federal espionage context will be examined. Fifth, the proposed computer crime legislation will be introduced and discussed in light of the previous discussion. Sixth, the felony copyright bill will be examined.

Finally, an analysis will be presented that concludes that the evolving state and Federal notions of property cover software and information, and that the taking of information rises to the level of "damage" under the proposed computer crime bill. Thus, a single unauthorized taking of information may rise to the level of a felony under S. 1322 while under S. 893 multiple occurrences of copyright violations may be required to rise to the level of a felony.

This protection for software owners is unprecedented and far exceeds that offered in the European Community. The proposed computer crime law, however, is not so sweeping as to unreasonably limit reverse engineering. The law is focused solely on criminal, not competitive,

behavior. The proposed computer crime law, should it be reintroduced and become law, will become a necessary but powerful tool in the legal arsenal against computer crime and software piracy. This arsenal would become further strengthened by enacting a new Federal Trade Secrets
Act based on existing state trade secret laws. This act would help further protect the rights of software owners and licensees by prohibiting the taking and use of trade secrets embodied in computer software or data.

II. AN OVERVIEW OF COMPUTER CRIME

The issues in controversy at the heart of computer crimes are theft of computer software and information, and the gaining of unauthorized access. In order to more fully understand the legislative and judicial responses by the states and the Federal government, one should first be aware of some incidents of computer crimes.

It has been stated in open forum that

> [j]ust as a kid enters another's property is trespassing, or who goes into another's home is breaking and entering, or who steals another's apple . . . is stealing, so, too, a hacker who manipulates or destroys a computer program of another or who renders it inoperable is breaking the law. As a society, we can't tolerate that.[1]

Computer crime costs U. S. businesses as much as five billion dollars per year; individual incidents average $450,000.[2] Computer crime, from a investigatory point of view, is sui generis. By their very nature, computer crimes often leave no evidence.[3] Therefore, the legal emphasis must be placed on being able to prove knowledgeable intent and damage.[4] Another facet of computer crime is its stealth and frequency. The incidence of computer crime is much higher than one may think. Most violations may never be reported. The following is a representative sampling of some notorious incidents of computer crime.

Shadow Hawk[5]

A young man was recently prosecuted for breaking into American Telephone and Telegraph (AT&T) and United States Government computers. Herbert W. Zinn was fined $10,000 and sentenced to nine months in prison under 18 U.S.C. § 1030(a)(4). After successful attempts to break into computer systems and retrieve proprietary data and software, Zinn, using the handle "Shadow Hawk," boldly advertised his proven techniques on public computer bulletin boards.[6]

Cornell virus / INTERNET Worm[7]

A computer virus is

> any computer program not readily discernible to the user that has the capacity to infect other computer systems by recreating itself randomly or causing some other specific action in some predetermined circumstance.... The effect can range from being nearly harmless to being devastating, . . . viruses can begin the infectious process from a home personal computer, an office, an academic institution, or from almost anywhere in the world.[8]

Once a computer is infected with a computer virus, it will infect other computer systems that are connected to it or diskettes that come in contact with an infected computer system.[9] In November, 1988, Robert Tappan Morris, a graduate computer science student at Cornell University, introduced a computer virus into a nationwide computer network known as INTERNET. [10] The virus searched for computers on the network that used the "UNIX" operating system as their master program. It then replicated itself within each of these computers while it searched for access routes to still other computers connected to the victim computers. It did not erase information but caused all affected computers to slow down to the point of uselessness.[11] The INTERNET virus was apparently meant as a harmless prank. As many as 6,000 computers, however, were disabled and as many as 10,000 people could not be productive for two days.[12] On January 22, 1990, Morris was found guilty of Title 18, U.S.C., Section 1030(a)(5) in U.S. District Court in Albany, N.Y.[13]

A virus similar to the INTERNET virus has made frequent appearances. In December, 1987, a seemingly innocuous Christmas message was deposited into the global electronic mail system (email) of International Business Machines, Inc. [14] This message was in reality a worm that presented a simple Christmas Tree on the display terminals of some users.[15] While it did this, it scanned the user's mail list and sent this holiday message to those users. Within a short while, so many messages were being created and sent that the entire system was disabled for a few days.[16]

German Hacker [17]

From 1986 to 1987, German (then West German) hackers were tracked searching though computers connected to MILNET. The hacker, Marcus Hess, had been scanning files relating to the Strategic Defense Initiative (SDI).[18] Dummy information was planted in MILNET so that the hacker would continue his forays while an investigation commenced. A cooperative effort consisting of Mr. Clifford Stoll, Lawrence Livermore Laboratory, the FBI, and the Air Force Office of Special Investigations tracked the hacker to Hannover, Germany.[19] Clearly, the networks of the United States are actively searched for any and all information

that can be used to the detriment of its national interest. Global computer espionage must be anticipated as a daily occurrence on these networks.[20]

Other Instances of Computer Crime

* An individual who designed and introduced a virus into a computer system thereafter attempted, through an attorney, to sell a remedy for the virus to the Federal Bureau of Investigation.[21]

* A disgruntled former employee sent a diskette to his old employer. This disk contained the "Scores" virus and caused serious damage to the former employer's computer when it was inserted into the system.[22]

* A physician sent a diskette to various health institutions throughout the world, ostensibly as a source for AIDS information. Use of the disk caused serious data loss. The physician later attempted to extort money from victims and potential victims by offering advice on how to recover lost data.[23]

* A hacker, Robert Mitnick, plead guilty in 1988, to numerous instances of hacking rising to the level of fraud in violation of 18 U.S.C. § 1030(a) (4).[24]

* Members of the underground hacking group "Legion of Doom," such as Lynne Doucette, have stolen more than $650,000,000 worth of telephone access time.[25]

* Three men, Kevin L. Poulsen, Mark K. Lottor, and Robert E. Gilligan, broke into U.S. Government and telephone company computers and had access to classified military flight orders.[26]

* A university computer expert blackmailed a former employer in order to extract payment that he thought was due him. U.K. university lecturer Dr. Roy Booth, 27, was fined £1,000 after threatening the firm with a computer virus that was to destroy a £200,000 computer program.[27] Clearly, the incidents of computer crime have been diverse. Not surprisingly, their scope, cost, and frequency have given rise to legislative and judicial responses on the state and Federal levels.

III. LEGISLATIVE AND JUDICIAL RESPONSES TO COMPUTER CRIME[28]

In Mahru v. Superior Court,[29] the Court declared that if an employee has permission to access an employer's computer for fraudulent acts, the charged employee may use this authorization as a defense against prosecution in that case.[30] Perhaps as a result of decisions such as these which bring to light the shortcomings of state statutes and the frequency of

computer crimes mentioned above, states have become very proactive in enacting computer crime legislation.[31]

States which modernized their laws by explicitly including computer programs within the scope of property include Alabama,[32] Arizona,[33] Arkansas,[34] California, [35] Colorado, [36] Florida, [37] Hawaii,[38] Idaho,[39] Illinois,[40] Iowa,[41] Kansas,[42] Louisiana[43] Minnesota,[44] Mississippi,[45] Missouri,[46] Nebraska, [47] New Hampshire, [48] New Mexico, [49] North Carolina,[50] Oklahoma,[51] Oregon, [52] Pennsylvania, [53] Rhode Island,[54] South Carolina,[55] Utah, [56] Virginia,[57] West Virginia, [58] Wisconsin,[59] and Wyoming.[60] States which merely penalize the unauthorized transfer of computerized information under certain circumstances include Alaska, [61] Connecticut,[62] Delaware,[63], Georgia,[64] Indiana,[65] Kentucky[66] Maine,[67] Maryland,[68] Michigan,[69] Nevada,[70] New Jersey,[71] New York,[72] North Dakota,[73] Tennessee,[74] and Texas.[75] Massachusetts is moving towards implementing a computer crime bill.[76] Current Federal law covers aspects of computer crime such as the fraudulent use of access devices,[77] fraud by wire,[78] the prohibited use of interception devices,[79] access to restricted atomic data,[80] and unlawful access to stored information.[81] The most comprehensive legislative act enacted thus far was the Computer Fraud and Abuse Act of 1984.[82] This was followed by the Computer Security Act of 1987.[83] A recent legislative proposal, however, would be the most encompassing. Senate Bill 1322 has recently been proposed and would criminalize computer tampering, destruction, and other damage.[84]

IV. SOFTWARE AS PROPERTY: THE EVOLVING VIEW

Crucial to successful prosecutions for computer crimes is proving damages. Often times, the "damage" that occurred was the removal of data or programs from a victim's computer systems. Several defendants have argued that computer programs are not property under the traditional common law definition of property, and thus the taking of data and software cannot rise to the level of conversion or theft. State courts, however, have generally been quick to revise the common law definition of property to include intangible property such as computer programs. This movement, combined with the strong efforts to codify an expanded definition of property by a majority of the states, discussed above, have resulted in a general consensus that software and information is property for purposes of theft and conversion. A survey of several state and Federal cases demonstrates the trend to widen the definition of property, a term whose parameters under earlier common law had excluded information and data.

A. United States v. Robert J. Riggs and Craig Niedorf[85]

This court accepted the argument that computer software was of such a nature to be transported in interstate traffic. Robert Riggs and Adam Grant, both members of the underground hacker group "Legion of Doom," plead guilty on July 9, 1990, of stealing

proprietary software, The court declined to accept the defendant's pretrial arguments that the stolen software, a "911 " emergency telephone switching software program, was not tangible property and could not be stolen.[86] Importantly, the Northern District of Illinois determined that confidential information rises to the level of property for purposes of wire fraud, 18 U.S.C. § 1343, and interstate transportation of stolen property, 18 U.S.C. § 2314.

B. United States v. Seidlitz[88]

Bertram E. Seidlitz used his knowledge of his former employer's computer system to enter the system surreptitiously, through the telephone lines, and remove copies of proprietary computer programs. His former employer was engaged in the design of sensitive computer software systems for U.S. Government clients. In a prosecution for fraud by wire, the court held
that there was sufficient evidence from which a jury could find that information stored in computer system was "property" as used in 18 U.S.C. § 1343.[89]

C. United States v. Kelly[90]

David E. Kelly and Matthew Palmer, Jr. used their employer's computer resources to design a software system for their own personal and pecuniary benefit. The defendants challenged the prosecution on the grounds that they did not derive any money or other economic gain. The court refused to restrict the construction of the relevant wire fraud statute, 18 U.S.C § 1341, denying the defendant's assertion that unauthorized use of information is not the taking of property sufficient to justify prosecution under the statute. This result was deliberately consistent with the Eight Circuit decision below.

D. United States v. States[91]

The Kelly court referred to United States v. States for its support. In States, the defendants were indicted on multiple counts of mail fraud. The States court held that neither the language of the statute nor its legislative history suggested the limitation of fraud only to situations concerned with money or purely tangible goods. The court felt that to restrict the reach of the statute served only to the deprive owners of tangible property interests.[92] Kelly fully supports the expansive view of property expounded in States.[93]

E. United States v. Paul A. Lambert[94]

Defendant Lambert was an employee of the Drug Enforcement Administration (DEA) in Washington, D.C. Lambert was charged with selling restricted information, contained within a DEA computer, detailing the identity of informants and the status of drug traffic investigations. Lambert was guilty of violating 18 U.S.C. § 641.[95] It was undisputed that only information was transferred; no tangible property of any kind, even documents, were

transferred.[96] The court needed to determine whether information was a "good" within the scope of § 641. After determining that the legislative history of § 641 was inconclusive, the Lambert court looked to prior cases to determine whether information could be considered a thing of value. It accepted the Second Circuit's decision, below, that information was a good.

F. United States v. Bottone[97]

The Second Circuit Court of Appeals interpreted a statute prohibiting the interstate transportation of "any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted, or taken by fraud."[98] The defendants removed documents describing a valuable chemical process. The documents were copied at another location and notes were made; the originals were returned unharmed. The copies, not the originals, moved through interstate commerce.

The issue facing the Bottone court was whether the copies were "goods" within the meaning of the § 2314. The court concluded that copies were within the definition of "goods. " The Bottone court reasoned that "where the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial.99 Apparently, a failure to reduce the information to another writing might well be a fatal flaw in a § 2314 prosecution. Section 2314, however, is narrower in scope than § 641. Thus, if information was a good under 2314, it is more likely that it should be deemed to be a good under § 641.

In addition to looking at Bottone, the Lambert court also looked at United States v. Rosner.[100] In Rosner, the defendants were charged under § 2071 with removing grand jury minutes from the U.S. Attorney's Office in the Southern District of New York.[101] The Rosner court concluded, however, that § 2071 did not apply since the documents were neither impaired nor destroyed.

In United States v. DiGilio the defendants were prosecuted for photocopying FBI records and selling them to subjects of investigations.[102] The DiGilio court rejected as unnecessary the Government argument that the deprivation of exclusive possession of the information contained in the records violated § 641. Since DiGilio made these copies during office time, with government machines, and on government paper, the copies themselves were government property. The court cautioned, however, that it did not imply a rejection of the government's broader interpretation of § 641.[103] In fact, the Third Circuit mentioned that any prosecution for theft of government information, rather than of the documents themselves would probably rise to the level of a "thing of value" in § 641.[104]

After considering Bottone, Rosner, and DiGilio, the Lambert court saw no reason to restrict the scope of § 641 only to the theft of government paper and ink or to unauthorized

reproduction.[105] The phrase "thing of value" in § 641, in conjunction with the explicit reference to "any record," covers the contents of the applicable records.[106] This finding is consistent with a similar determination in United States v. Friedman.[107]

G. Hancock v. State[108]

Robert F. Hancock was charged with the theft of fifty-nine computer programs from his employer under the applicable Texas state theft statute. Hancock had intended to sell the programs to a competitor of his employer. Under the then applicable Texas code, "property," as used in the crime of theft, included "[a]ll writings of every description, provided such property possesses any ascertainable value."[109]

In an issue of first impression, the Hancock court concluded that the relevant computer programs are property that came within the scope of Texas' statutory definition of theft.[110]

H. National Surety Corp. v. Applied Systems, Inc.[111]

Max G. Coffey and Robert S. Sawyer converted a fifty-eight program computer payroll system belonging to their employer, Applied Systems, Inc., to their own use. National Surety Corporation was found liable on a liability bond. The defendants were charged under the applicable Alabama criminal law.[112] Unlike Texas, however, there was prior authority stating that intangible personal property can be the subject of larceny.[113] As a result, the court held, in part, that intangible personal property can be converted, and that was the issue before the National Surety court.[114]

The court also referred to Alabama's Criminal Code which defines "property" as "[a]ny money, [or] tangible or intangible personal property ...."[115] A contrary determination on the theft of intangible property would be inconsistent. It would mean that intangible personal property can be subject to theft and yet not be subject to conversion [116]

I. Indiana v. McGraw

Michael McGraw was charged and convicted by a jury of two counts of theft of the use of computer services. McGraw used a computer at his place of employment to keep accounting records for a personal, unrelated business.[118] The determination of whether the use of computer equipment is property for the purposes of theft was an issue of first impression.[119] After reviewing the determinations of Hancock, National Surety, and Helvey v. Wabash County REMC,[120] the court determined that computer time is "services" for which money is paid.[121] These services may reasonably be regarded as valuable assets. Thus, computer services are property within the meaning of the definition of property subject to theft.[122] The court held that the offense was complete and the conviction proper.[123]

J. Contrary Authority

1. Lund v. Commonwealth[124]

Charles Walter Lund was charged with both theft of computer equipment, supplies and access time in violation of Virginia Law.[125] Lund was a graduate student who had used tens of thousands of dollars worth of computer time without prior authorization in the pursuit of his Ph.D. research in statistics.[126] It was uncontroverted that he would have been given access to the computer services had he asked for it.[127] He was subsequently convicted of grand larceny and sentenced to probation.[128]

The Lund court proceeded under the premise that criminal statutes must be narrowly construed.[129] Thus, the Lund court reasoned that the phrase "goods and chattels" cannot be interpreted to include computer time and services. Since the word "use" does not appear in the Virginia Code covering larceny, the unauthorized use of a computer cannot be larceny.[130] The court declared that the "language of the statutes connotes more than just the unauthorized use of
the property of another. It refers to a taking and carrying away of a certain concrete article of personal property."[131] In the end, the Lund court held that the unauthorized use of a computer cannot be construed to be subject of larceny under Virginia Law, reversed the conviction of Lund, and quashed the indictment.[132]

2. People v. Weg[133]

Theodore Weg was charged with the Class A misdemeanor of theft of services for using his employer's, the Board of Education, computer for his own personal benefit and without his employer's permission.[134] The central issue facing the Weg court was whether computer time was "business, industrial or commercial" equipment within the scope of the statute.

Citing legislative history (the statutory provision was meant to close a loophole in commercial law), and legislative interpretation conventions (words are to be interpreted within their immediate context)l and prior judicial practice (that "commercial" may be deemed not to include governmental, not for profit activities), the court held that the statute could only be interpreted as covering only for profit activities.[135] The court dismissed the information against Weg.

In reviewing these two contrary cases, it is clear that both do not now represent the current status of the law in either jurisdiction. The Lund court read the Virginia law extremely narrowly, and reached to fifty year old analogies where more contemporary analogies were available. It seems that the Lund court went out of its way to exclude computer access time from property perhaps due to the nature of crime and the context of the defendant's activities.

Lund remains a contrary and minority position, perhaps limited to its particular facts. Much of the same criticism can be made of the Weg decision by the New York court.

Subsequent to these decisions, however, both Virginia and New York have enacted laws that prohibit the unauthorized taking of computer data and services.[136] Thus, it seems clear that the most contrary judicial decisions standing in the way of classifying computer programs and access time as property seem to have been superseded by decisions by the applicable legislatures. The act enacted by Virginia is very much consistent with the judicial positions taken by the majority of state courts rights in computer software and services. The affirming property New York law, enacted in 1986, is a good first step by punishing the destruction of data or its integrity. The majority of the aforementioned cases protect a software owner's or developer's property interest. Clearly, there is a strong trend to declare computer software and computer access as property. This property interest is sufficient to rise to the level encompassed by statutes dealing with theft, conversion, and larceny. Once this property interest has been implicated in these statutes, damages must be ascertained. Where data or software has been stolen or converted, damages have been found to include the value of the information taken or the services used. Once damages are determined, all that remains to be done to attain a successful prosecution is demonstrating the requisite intent.

V. INFORMATION AS PROPERTY: THE FEDERAL VIEW IN ESPIONAGE CASES

The issue of information as property is not only discussed in forums concerned with computer crime. Federal espionage cases often turn on whether sensitive information is of sufficient substance to be a "thing" within the purview of Federal espionage law. In the espionage context, information has been deemed an item of value, the mere taking of which violates Federal law. This notion has significant consequences when interpreting the damage requirements of the proposed computer crime bill, to be discussed below. The most celebrated case involving the issue of information as property was **United States v. Samuel Loring Morison.**[137]

Samuel Loring Morison was employed as a naval warfare analyst at the Naval Intelligence Support Center (NISC) just outside Washington, D.C. from 1974 to 1984. Morison held "Top Secret-Sensitive Compartmented Information" security clearance and worked in a "vaulted area" closed to all without a Top Secret clearance. Morison sent one classified reconnaissance photograph to an international publisher of defense information.[138] In return, Morison received a few hundred dollars for his efforts.[139] The publisher, Jane's Defence Weekly, apparently had no knowledge of the classified nature of the photograph. Morison was tried and convicted under 18 U.S.C. § 641, and 18 U.S.C. § 793(d) and (e). The Fourth Circuit affirmed Morison's conviction.[141]

18 U.S.C. § 641, a statute proscribing the theft of government property, provides that whoever "knowingly converts to his own use or the use of another, or without authority conveys . . . any record . . . or thing of value of the United States" is guilty of a felony if the value of the property exceeds $100. One of the issues facing the court was whether information contained in classified documents is a "thing of value" for purposes of § 641. The Morison court held that § 641 applies to the conversion of secret Navy documents and photographs.[142] The court looked to Carpenter v. United States.[143] Based, in part, on the Carpenter decision, the Morison court declared emphatically that information "constitutes property which may be the subject of statutory protection under section 641,..."[144]

In a subsequent and similar case, United States v. Fowler,[145] Richard Lee Fowler used information from classified reports to prepare unclassified reports for his employer, Boeing. He was charged under 18 U.S.C. § 641. The Fowler court also looked to prior decisions regarding the nature of information as a thing of value. Both the Morison and the Fowler courts saw the issue as settled due to a recent Supreme Court decision.

In Carpenter,[146] the Court held unanimously that the intangible nature of a newspaper's confidential business information did not "make it any less 'property' protected by the mail and wire fraud statutes."[147] Following this reasoning, the Fowler court stated that even if Fowler were charged with conversion of information only, § 641 would still "apply because information is a species of property and a thing of value."[148] In affirming the conviction of Fowler, the court agreed with the Second and Sixth Circuits that "conversion and conveyance of governmental information can violate § 641."[149]

Clearly, mere information can be converted under Federal law. It seems that only the value of the appropriated information may be most in controversy. In future litigation, defendants may want to concentrate their defense on the value of the information transferred. In Morison, the court acknowledged that Morison did not bring in experts on the value of the relevant information to rebut the government's assertions that the value of the information taken rose above the statutory floor.[150] This may have been a serious oversight by Morison. Just what is the value of information to the government when the information itself reveals neither nothing new nor exposes no hitherto unknown methods or sources to the public or to adversaries was never addressed.

VI. COMPUTER CRIME LEGISLATION: S. 1322

The latest comprehensive crime bill incorporates S. 1322, the Computer Abuse Amendments Act of 1991, sponsored by Senators Leahy, Brown, and Kohl, and introduced on June 18, 1991.[151] The Computer Abuse Amendments Act of 1992 was an amendment to H.R. 3349 (S. 1322 in 102nd Congress). S. 1322 passed the Senate as an amendment to S. 1241, the Violent Crime Control Act. It was altered slightly in conference with the House in

November, 1991. It passed the House as part of the conference report to H.R. 3371, the Violent Crime Control Act. The provisions of S. 1322 were changed slightly in conference and can be found in the conference report. The final form of S. 1322 can be found as the title dealing with computer crime in the conference report on H.R. 3371. For simplicity, however, the computer crime provisions will be referred to in this paper as S. 1322.

The proposed bill would have amended 18 U.S.C. § 1030(a)(5) to punish the knowing or reckless causing of a transmission of a program into a computer used in interstate commerce if the person causing the unauthorized transmission intends that damage occur or that access to the computer system is denied others. There must be resultant damage that exceeds one-thousand dollars over any one-year period, or impairs in any way the medical treatment of any individual.

While the bill did not succeed the 102nd Congress, the Senate Judiciary Committee fully intends to resubmit the computer crime provisions, if not the entire crime bill, during the 103rd Congress[152]. While there has been no opportunity to interpret provisions of the bill, the concept of damages in a computer and/or information context has been discussed in both state and Federal courts. Thus, the Federal courts will have considerable jurisprudence on the matter should they be faced with an issue requiring an interpretation of the damage provision of an amended § 1030(a) (5).[153] By interpreting the amended § 1030(a)(5) consistently with prior computer crime cases, one quickly realizes that the scope of the amended law may be greater than that provided by recently passed felony copyright legislation in a computer software context.

VII. FELONY COPYRIGHT LEGISLATION; S. 893[154]

A. Overview of Senate Bill 893

S. 893 amends Section 2319(b) of Title 18 of the United States Code relating to criminal penalties for copyright infringement. S. 893, the Software Copyright Protection Bill, was sponsored by Senator Orrin Hatch (R-Utah) and originally passed the Senate on June 4, 1992. Representative William Hughes (D-New Jersey), chairman of the House Intellectual Property and Judicial Administration Subcommittee, reported the bill out on September 30, 1992. It passed that chamber by voice vote on the night of October 3, 1992. Thereafter, on October 8, 1992, the Senate unanimously agreed to the House version. The bill was signed by President George Bush on October 28, 1992, and became Public Law 102-561.

The bill is strongly endorsed by the Software Publishers Association (SPA), an indu. trade group,[155] and Nintendo of America, a recreation software distributer.[156] The law defines commercial pirates as those who willfully copy software for commercial advantage or private financial gain. Prison terms of up to five years and fines of up to $250,000 may be imposed on

those convicted of infringing at least ten copies of a copyrighted software program or any combination of programs with a retail value greater than $2,500. Repeat offenders can face up to ten years' imprisonment.[157] Notably, the law does not encompass an individual who makes one copy of a program for personal use or to share with another. It is clear that S. 893 is meant to protect software developers only against persons who copy and then sell computer software on a commercial basis. The law would provide protection that is consistent with anti-piracy protection already granted to the motion picture and sound recording industries.

It is estimated that software piracy in the U.S. alone cost the software industry more than $2.4 billion in 1990.[158] Global losses resulting from the unauthorized copying of software exceed $10 billion.[159] The SPA cited three bases for support of the bill before the House Subcommittee on Intellectual Property and Judicial Administration. First, SPA Executive Director Ken Wasch, while extolling the health of the software industry, declared its vulnerability to software piracy due to the very nature of software. He declared that

> [the software industry is] the only industry that empowers each and every customer to act as his own manufacturing subsidiary.... Anyone with a standard personal computer can make an unlimited number of identical perfect copies of a program. This leaves us especially vulnerable to the most rapacious forms of commercial piracy.[160]

Second, the current legal regime only provides for misdemeanor penalties and weak civil remedies; these are not sufficient to deter software pirates. Software pirates are masterful at avoiding legal process, discovery, and seizure when faced with a civil complaint. No civil damages were collected in a recent multi-million dollar counterfeit software case as there were woefully insufficient business records to justify an award.[161]

Finally, there has been a marked lack of effort in enforcing software property laws due to a reluctance on the part of law enforcement. Wasch opines that "it is very hard to persuade an overworked federal attorney to commit scarce public resources to a technical investigation that can only result in a misdemeanor conviction. With its felony penalties, S. 893 gives law enforcement the incentives it needs to battle software pirates."[162] The new copyright law declares that willful infringement for commercial advantage or private financial gain is punishable according to the provisions of 18 U. S.C. § 2319.

The pre-amended § 2319 "allows felony penalties of up to five years imprisonment and/or a $250,000 fine for anyone who, within any 180-day period, illegally reproduces or distributes at least one-thousand copies of a copyrighted sound recording or at least 65 copies of a copyrighted motion picture or other audiovisual work."[163] For more modest unauthorized copying, lesser penalties apply. Consequently, activity resulting in more than one-hundred but less than one-thousand copies of sound recordings or eight to sixty-four copies of motion pictures made within the statutory period of 180-days results in a penalty of only up to two

years and/or $250,000. Other criminal copyright infringement is merely a misdemeanor punishable by up to one year of imprisonment and/or $25,000.

An earlier version of the felony copyright bill would have amended Section 2319(b)(1) so that it would impose up to five years imprisonment and/or a $250,000 fine for those who make more than fifty copies of one or more computer programs during any six-month period. For other infringements involving more than ten but less than fifty copies an amended Section 2319(b)(2) would have provided up to $25,000 fine and up to one year of imprisonment.

The final bill, however, gives equal protection to all classes of copyrighted material. The finalized penalties under the amended bill now include:

(1) up to five years imprisonment for at least ten improper copies made during a 180-day period where the copies have a retail value in excess of $2,500, and

(2) up to ten years of imprisonment for a second or subsequent offense, and

(3) up to one year of imprisonment in any other copyright infringement cases.[164]

The fine provisions of this law would be determined, according to one source, by the provisions of 18 U.S.C. § 3571-74 and the Uniform Sentencing Guidelines, § 2B5.3, 5E1.2.[165] These provisions recommend a maximum fine of $250,000 for individuals and $500,000 for organizations.

It must be noted, however, that some industry spokesmen expressed concern that S. 893 would expose reverse engineering of programs to felony penalties. This bill is, however, designed neither to

> infringe[] on traditional concepts permitting fair use of copyrighted materials for purposes of research, criticism, scholarship, parody, or other long recognized uses.... [nor] designed to interfere with evolving notions of fair use, as that concept is applied with respect to new communications networks and computer technologies[166]

It is hoped that this traditional fair use would continue to apply to reverse engineering, customer service, and scholarship, all of which foster competition and not the reaping of pecuniary benefits entitled to another.

B. Comparison With the European Community Position

Britain's 1988 Copyright, Designs and Patents Act, containing both civil and criminal provisions, is the most detailed legislation on software copyright in the European Community. Parts of a recent European Community (EC) Directive were modeled on this law. It calls upon

EC member nations to provide copyright protection for computer software but only allows "reverse engineering" in specific circumstances.[167] Compromising as the directive is, however, the U.K. implementing legislation has been sharply criticized for providing even less explicit protection for software developers than was vigorously negotiated for in Brussels.[168]

A strong EC directive would benefit developers. It appears that there is significant evidence that a legal regime protective of software rights lowers the incidence of software piracy.[170] When one reviews the dollars lost to software piracy, one quickly realizes that the nation with the least loss per personal computer, the United Kingdom, is the nation with the most stringent anti-copying regime.[171]

The proposed U.S. legislation concerning protection of computer software rights is more stringent than the E.C. directive, and certainly more demanding than the proposed U.K. implementing legislation. The U.S. bills on computer crime and felony copyright will represent the cutting edge in software protection.

VIII. CONCLUSION

A. With Information Considered as Property, The Taking of Which is Conversion, Unauthorized Copying of Data or Software Rises to the Level of Damages Under Proposed S. 1322, A Result Exceeding That of S. 893.

To find a felony conviction under the proposed computer crime statute, the United States must prove that an unauthorized command or program was transmitted intentionally or with reckless disregard through interstate commerce into a computer system. This activity must result in damage to the computer system in excess of one-thousand dollars. In interpreting "damage" a Federal court may first refer to the several Federal and state cases discussed as persuasive evidence for the proposition that information and data, in and of itself, are capable of being converted.[172]

A survey of some Federal cases discussed above clearly supports the view that information, regardless of copyright status, can be converted for purposes of criminal theft and wire fraud law. United States v. Riggs and Niedorf stands for the proposition that information is property under the wire fraud and theft laws.[173] United States v. Seidlitz declares that computerized information is property under the wire fraud statute.[174] United States v. Kelly asserts that the unauthorized use of computerized information is sufficient to rise to the level of a taking of property.[175] United States v. Lambert held that the mere taking of information violates § 641.[176]

State cases also demonstrate a strong pattern supporting the assertion that the taking of information from computer systems rises to the level of a crime under state conversion

statutes. Hancock v. State,[177] National Surety Corp. v. Applied Systems, Inc.,[178] and Indiana v. McGraw[179] all support the view that either computer access or computer information are either property or services that, if appropriated improperly, may be punished under applicable state theft and conversion laws.

Once having ascertained that information, regardless of its copyright status, rises to the level of property, the court can then turn to the issue of whether the taking of information and data, a form of intangible personal property, rises to the level of damage. The cases supporting this view include United States v. Morison,[180] Carpenter v. United States,[181] and United States v. Fowler.[182] In these and other cases discussed above, the courts again supported the view that mere information rises to the level of property, the taking of which results in damage to the United States.

Thus, under proposed S. 1322, one who uses a program or code to enter a computer used in interstate commerce, without authorization, and copies or otherwise appropriates data or information, causes damage for purposes of S. 1322 if damage is interpreted consistent with current state and Federal conversion and espionage laws. The issue of whether the information taken or copied is copyright protected is not a central issue under a S. 1322 scenario, though this information may relate to a showing of the value of the damage done. Under this interpretation of damage, the greatest issue remaining is the dollar value of the damage. This, however, will often be a question of fact. Nonetheless, the value of the damage will not be limited to the physical harm caused under activity proscribed by S. 1322 but will surely include the cost of the creation or the cost of the release of the information copied or appropriated.

One can easily describe a scenario that results in liability under S. 1322. A computer hacker or pirate uses the phone lines to gain access to a computer or computer network used in interstate commerce. The actor uses a code or program he or she is not authorized to use, and intentionally copies information and data that is not copyright protected. The actor copies information from the computer system that consists of a small program worth $1,000 on the open market and copies numerous valid computer "log-on" passwords. The information in this scenario cost at least $1,000 (e.g., the market value of the computer program) and also will result in expenditures of at least $1,000 in preventative action due to the release of the information (i.e., the deleting and changing of computer log-on passwords and concomitant personnel costs to accomplish this task). This actor has now satisfied all requirements for prosecution under proposed S. 1322 and its version of 18 U.S.C. § 1030(a)(5)(i) and (ii).

Thus, one instance of a taking of information, whether software or not, whether copyrighted or not, rises to the level of damages under S. 1322. This result would be consistent with numerous Federal and state cases and statutes, discussed above, that have found damage for the mere unauthorized using of information or the copying of information.

Under a wide reading of damages under S. 1322, more protection is offered the owner of data and information than is provided by S. 893 in a computer software copyright context. Under S. 893, the appropriated work needs to be copyrighted, while the violation needs to be egregious or repeated. Under S. 1322, the data, information or program need not be copyrighted, need only be appropriated once, and need only break through a lower minimum floor of damage. This is certainly more protection than is available in other nations such as the recent EC Directive on computer software.

B. A Proposal For a Federal Trade Secrets Act

As only the felony copyright bill survived the 102nd Congress, consideration of the computer crime bill is likely in the 103rd Congress. The 103rd Congress, should, in conjunction with review of the computer crime measures discussed, consider a new, criminal Federal Trade Secrets Act. Federal trade secrets law may help prevent the use or taking of computer programs by computer criminals and industrial saboteurs not only within the United States but abroad as well. A new Federal trade secrets law, generally modeled on existing state trade secret laws,[183] would be within the power of Congress under the Commerce Clause of the U.S. Constitution.[184] The Federal version, though, would have provisions concerning computer programming, computer information and technology, and regulations concerning extra-territorial restrictions on use of trade secrets embodied within computer programs and access to Federally protected trade secrets by both U.S. citizens and foreign nationals regardless of the geographic location of the person at the time of the criminal act.

A trade secret is any form of information that gives a firm an advantage over competitors who are not aware of the secret.[185] It is crucial that trade secrets be protected from disclosure to the public or they lose protection under the various state trade secret laws.[186] In a way, trade secrets protect relationships at least as much as they protect property. Once the trade secret becomes known, it no longer has value to a firm. What the trade secret laws seek to do is to ensure loyalty between an individual and a firm. When a person divulges trade secrets, that person
is liable for the breach of confidence, the dollar amount of which can only be determined through an extensive examination of each case.

A Federal trade secrets law, therefore, would enforce, through potential prison terms and substantial fines, a confidential relationship between an employee of a firm and their employer or punish the taking or use of computer programs and data embodying trade secrets. In a corporate context, combined with specific and documented corporate rules and regulations, employees would be prohibited by strict Federal law from transferring Federal trade secrets and computer programs abroad or from divulging trade secrets to anyone not authorized by the Company.

The new law should have clear and explicit extraterritorial application to be effective in preventing computer crime which originates or is continued overseas. This would not only be consistent with the concept of extra-territorial application of antitrust,[187] securities laws,[188] and rules of civil procedure,[189] but would also be properly applied against those with notice of extra-territorial application.[190] That is, those seeking the protection of the Federal trade secret law must, as an organizational entity, acknowledge the extra-territorial application of the Federal trade secret law. This is frequently the case with forum selection,[191] choice of law,[192] and arbitration clauses in international contracts.[193]

A new Federal trade secrets law can work in tandem with the new felony copyright legislation and a future computer crime act. A Federal trade secret law protecting computer programs can also work with new revised export restrictions which restrict the export of sensitive computer programs without the permission of the software owner or licensee and, at times, the United States Government. Current export restrictions are found in the Export Administration Act,[194] the Arms Export Control Act,[195] the Defense Industrial Security Program (DISP),[196] and the Trading With the Enemy Act.[197] A Federal Trade Secrets Act, combined with proposed computer crime and the new felony copyright legislation, should prove to be a most effective combination of legislative tools in opposing computer crime and computer criminals. Further, by proscribing computer crime abroad, a Federal Trade secret Law would provide a vehicle of enforcement against future Hannover-like computer espionage attempts.

IX SUMMARY

As a result of increased occurrences of computer crime, of its notoriety, and its costs, there have been numerous legislative and judicial responses. Most notably, there has been a strong trend in state legislatures and in state courts to consider computer software, data and access as property. The theft of software, even of making copies of software or data, has been held to give rise to damages for purposes of state theft and conversion laws. There is a parallel trend in the Federal judiciary. This is especially so in the area of espionage. Where the issue of information as property has often arisen it is now settled policy that information can be appropriated for purposes of theft.

The recently proposed computer crime act, S. 1322, proscribes conduct that causes damage due to unauthorized or improper access of a computer system. In interpreting these provisions, should they be reintroduced and passed, Federal courts, in looking to prior interpretations of damages and information as properly, may properly determine that the unauthorized copying of data and programs easily satisfy the damage requirements of the proposed 18 U.S.C. § 1030(a)(5). This, in effect, would result in a Federal criminal penalty for a single unauthorized duplication of software or the taking of data. The potential sweep of

S. 1322 is broader in the area of software protection than that of the recently passed felony copyright legislation, S. 893.

Senate Bill 893 provides for criminal punishment for violations of copyrights, including software copyrights. Thus, criminal remedies that would have been available under S. 1322 under a liberal interpretation of its language are now granted explicitly in S. 893, but only if the converted data is copyrighted software or data and if the violation occurs repeatedly or is egregious.

It is clear that both these bills far exceed the protection granted in other nations. For example, the European Community Directive on software protection, years in the making, is not as sweeping as S. 1322 or S. 893. Yet, there is evidence that a strong enforcement regime does limit the occurrence, or at least the growth, of computer crime and software piracy.

While the proposed computer crime measure did not pass the 102nd Congress, it is likely that a similar package will be reintroduced in the current 103rd Congress. The public policy effects of this bill should be addressed so that its strong enforcement of software property rights does not run roughshod over the rights of developers, programmers, and academicians whose motives are proper and worthy.

In achieving the goal of limiting the theft of software, and, in light of the wide interpretation the courts may grant the proposed computer crime statute, Congress should be doubly sure to only target clearly criminal behavior, not software, hardware, customer support, or new development.[95] The statute, like the EC Directive, must explicitly allow reverse engineering in limited circumstances. There had been some concern that S. 893 would deny the right to reverse engineer a product. This same concern must be considered should an S.1322-like computer crime package be reintroduced in the 103rd Congress. Along with considering a new computer crime package, Congress should consider passing a new, criminal Federal Trade Secrets Act which would prohibit the taking or use of computer software or data that embody trade secrets, regardless of the location of the act.

It appears, however, that the proposed legislation directs itself to criminal behavior, requiring proof of knowledgeable intent and actual damages. S. 1322, while capable of punishing a single instance of the taking of another's data or software, punishes only criminal intent. Used to punish criminal activity and not to limit competition, customer support, or academic freedom, the proposed computer crime law, especially in combination with the felony copyright law and a new Federal Trade Secrets Act, should prove to be a thorough though sweeping legal regime fully responsive to the serious economic and security threats posed by computer criminals, industrial saboteurs and software pirates now operating globally.

Endnotes

1. The Impact of Computer Viruses and Other Forms of Computer Sabotage or Exploitation on Computer Information Systems and Networks, 1989: Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary, 101st Cong., 1st Sess. 2 (1989) [hereinafter Computer Virus Hearings] (opening statement of Sen. Patrick J. Leahy).

2. A Bill to Amend Title 18 of the United States Code to Clarify and Expand Legal Prohibitions Against Computer Abuse 1990: Hearing on S. 2476 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary, 101st Cong., 2nd Sess. 13 (1990) [hereinafter Computer Abuse Hearings] (testimony of the Department of Justice).

3. With a computer crime, there is no "crime scene. [T]hey are [] designed to self-destruct. Therefore, there is no evidence; there is no paper trail anymore." Computer Virus Hearings, supra note 1, at 29 (statement of Kenneth Walton). This is especially true when the unauthorized copying of software and data is concerned; often called software piracy.

4. Id.

5. Id. at 11, 32-33.

6. Computer Abuse Hearings, supra note 2, at 15; see also infra note 85 (discussing bulletin board related liability).

7. Computer Virus Hearings, supra note 1, at 5, 30, 86.

8. Id. at 10 (statement of William S. Sessions, director of the Federal Bureau of Investigation).

9. Id. at 64. This paper concentrates on how the legislative response to viruses may have created, in effect, a criminal computer software copyright law. For greater information concerning computer viruses than is presented here, see generally Robert V. Jacobson, The PC Virus Control Handbook (1992); Richard H. Baker, Computer Security Handbook (1992); Richard B. Levin, The Computer Virus Handbook (1992); Mark W. Greenia, Computer Security Information Sourcebook: A Guide for Managers Attorney's and Concerned Professionals (1992); Lance J. Hoffman, Rogue Programs: Viruses Worms and Trojan Horses (1992); Brenda Nelson, Note, Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm, 11 Computer/L.J. 299 (1991); Darryl C. Wilson, Viewing Computer Crime: Where

Does the Systems Error Really Exist?, 11 Computer/L.J. 265 (1991) (discussing state and Federal responses to computer crime and taking a somewhat more critical view of attempts to control computer crime); Robert J. Sciglimpaglia, Jr., Comment, Computer Hacking: A Global Offense, 3 Pace Y.B. Int'l L. 199 (1991) (also presenting a comprehensive comparative analysis regarding computer crime in Canada, the United Kingdom, and the United States); Anne W. Branscomb, Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime, 16 Rutgers Computer & Tech. L.J. 1 (1990) (also discussing computer crime and legislative responses); David R. Johnson, Thomas P. Olson & David G. Post, Computer Viruses: Legal and Policy Issues Facing Colleges and Universities, 54 Educ. Law Rep. 761 (1989); Michael C. Gemignani, What is Computer Crime and Why Should We Care?, 10 U. Ark. Little Rock L.J. 55 (1987); and John Montgomery, Computer Crime, 24 Am. Crim. L. Rev. 429 (1986).

10. Computer Virus Hearings, supra note 1, at 86. INTERNET, formerly called ARPANET, is a network composed of as many as 100,000 computers. Computer Virus Hearings, id. at 45. A similar network is known as MILNET, a military data network, allows access to authorized educational and research institutions. Id. MILNET, however, contains no classified information. Id. at 46. A computer network is comprised of two or more computers at different locations interconnected to an electronic communications system, such as the telephone system, for the purposes of data transfer. See Van Nostrand Reinhold Dictionary of Information Technology 136-39 (3d ed. 1989) (explaining the concept of data communications).

11. Computer Virus Hearings, supra note 1, at 65.

12. Id. at 57.

13. Id. at 40; see also United States v. Robert Tappan Morris, 928 F.2d 504 (2d Cir. 1991) (affirming conviction under 18 U.S.C. § 1030(a)(5)). The Morris court held, inter alia, that "the 'intentionally' standard applies only to the 'accesses' phrase of subsection 1030(a)(5)(A), and not to its 'damages' phrase." Morris, 928 F.2d at 509.

14. Computer Virus Hearings, supra note 1, at 87.

15. A worm is a virus that copies itself within a computer network. Id. at 52. The Cornell virus that Morris introduced into the INTERNET network is more correctly classified as a worm. Id. at 86. A similar destructive computer program is known as a "logic bomb." A logic bomb is a program that waits for a future event before it causes damage or confusion. Id. at 69. A "Trojan Horse" is a program that appears benevolent but injects harmful computer code once it is within a computer system. Id. at 86. A "bacterium" is computer code that replicates itself and interferes with computer

processors and memory. Id.

16. Id. 49-51 (analogizing this kind of attack as an electronic "ponzie scheme"). The worm had also sent account numbers, names, and passwords to clandestine destinations overseas. Id. at 52. Another INTERNET attack, originating once again at Cornell, occurred in 1992. See Cornell Computer Hackers, Accomplice Sentenced, UPI, Oct. 5, 1992, available in LEXIS, Nexis Library, UPI File.

17. Computer Virus Hearings, supra note 1, at 6, 87.

18. Computer Abuse Hearings, supra note 2, at 16. While Hess was tried and convicted, he was only sentenced to probation. Id.

19. Computer Virus Hearings, supra note 1, at 62-64.

20. Id. at 87.

21. Id. at 33.

22. Computer Abuse Hearings, supra note 2, at 14.

23. Id.

24. Id. at 15.

25. Id.

26. Id. at 49.

27. Computer Wizard Guilty of 'Virus' Blackmail, Press Ass'n Newsfile, Oct. 1, 1992, available in LEXIS, Nexis Library, CURRNT File. For additional cases, and the impact of computer crime investigations upon civil liberties, see David F. Geneson, Recent Developments In The Investigation and Prosecution of Computer Crime (1990) (PLI Order No. G4-3855); and Stanley S. Arkin, et al, Prevention and Prosecution of Computer and High Technology Crime (1991) (and sources cited therein).

28. The emphasis on this paper is on using the status of computer software and information as property to show that copyright violations and other unauthorized copying of data can rise to the level of computer crime under the proposed legislation. The paper does not cover copyright or patent protection for software outside of the issues presented herein. It should be noted that states, through trade secret laws, often have stronger protection over computer software violations than does existing Federal law. See infra note xx and accompanying text.

29. 191 Cal. App. 3d 545, 237 Cal. Rptr. 298 (1987).

30. Id. at 549, 237 Cal. Rptr. at 299.

31. For an informative survey of computer crime statutes, see generally, Daniel J. Kluth, Note, The Computer Virus Threat: A Survey of Current Criminal Statutes, 13 Hamline L. Rev. 297 (1990) (focusing on the Minnesota and Federal efforts).

32. Ala. Code § 13A-8-101(9) (1992). The act clearly supersedes the decision of the court in In re State of Alabama v. Central Computer Services Inc. Ex parte State of Alabama, 349 So. 2d 1160, 1163 (1977) (holding that computer software is not "tangible personal property for purposes of Title 51, section 788, Code of Alabama 1940 (Recomp.1958)."). As part of the court's analysis it looked to whether software had been treated as tangible property for tax purposes in prior cases; it had not been so treated. Id. at 1162-63. This issue is addressed well in Robert L. Cowdrey, Note, Software and Sales Taxes: The Illusory Intangible, 63 B.U. L. Rev. 181 (1983).

33. Ariz. Rev. Stat. Ann. § 15-727 (West 1991) (state government owned computer programs).

34. Ark. Code Ann. § 5-41-102(9) (1992).

35. Cal. Penal Code § 502(c)(1) (West 1992) (includes data among items that may be converted, in addition to money and property); id. § 502.01(a)(1) (programs are property subject to seizure).

36. Colo. Rev. Stat. Ann. § 18-5.5-101(8) (West 1991). Like all states that define programs as property, Colorado also punishes unauthorized access to computer systems. Id. § 18-5.5101(1) (stating that authorization requires express permission to use a computer system from a person who is authorized to grant this authority by their job description). Colorado's definition of "access" has been suggested as a model for Federal legislation. See Computer Abuse Hearings, supra note 2, at 33.

37. Fla. Stat. Ann. § 815.03(8) (West 1992).

38. Haw. Rev. Stat. § 708-890 (Michie 1991).

39. Idaho Code § 18-2201(7) (Michie 1992).

40. Ill. Ann. Stat. ch. 38, para. 16D-2(d) (Smith-Hurd 1992).

41. Iowa Code Ann. § 716A.1(8) (West 1992).

42. Kan. Stat. Ann. § 21-3755(1)(h) (1990).

43. La. Rev. Stat. Ann. § 14:73.1(9) (West 1992) (computer programs defined as intellectual property). For an analysis of Louisiana law, see Michael R. Testerman, Legal Protection of Computers: Trade Secrets Copyright and Newly Enacted Louisiana Statutes, 32 La. B.J. 290 (1985).

44. Minn. Stat. Ann. § 609.87(6)6 (West 1992).

45. Miss. Code Ann. § 97-45-l(i) (West 1991) (computer programs are intellectual property); id. § 97-45-l(j) (computer data, in any form, is property).

46. Mo. Ann. Stat. § 569.093(10) (Vernon 1992)

47. Neb. Rev. Stat. § 28-1343(13) (1991).

48. N.H. Rev. Stat. Ann. § 638:16(X) (1991).

49. N.M. Stat. Ann. § 30-45-2(E) (1992) (creates a new category of property, "computer property").

50. N.C. Gen. Stat. § 14-453(8) (Michie 1991).

51. Okla. Stat. Ann. tit. 21, § 1952(8) (West 1992) (presenting a very wide definition of property).

52 Or. Rev. Stat. § 164.377(h) (1991).

53. 18 Pa. Cons. Stat. Ann. § 3933(c) (1992).

54. R.I. Gen. Laws § 11-52-l(E) (Michie 1991).

55. S.C. Code Ann. § 16-16-10(f) (1991).

56. Utah Code Ann. § 76-6-702(5) (Michie 1992) (creates a new category of property, "computer property").

57. Va. Code Ann. § 18.2-152.2(3) (Michie 1992). For a still timely analysis of the Virginia laws, see Robin K. Kutz, Note, Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act, 27 Wm. & Mary L. Rev. 783 (1986).

58. W. Va. Code § 61-3C-3(n)(3) (Michie 1992).

59. Wis . Stat. Ann. § 943.70(h) (West 1991).

60. Wyo . Stat. § 6-3-501(ix) (1992) (programs are intellectual property); id. 6-3-501(x) (programs are property).

61. Alaska Stat. § 11.46.740(a) (1991).

62. Conn. Gen. Stat. Ann. § 53a-251(c) (West 1992) (theft of computer services); id. § 53a-251(d) (interruption of computer services). Connecticut case law, however, indicates that proprietary information is property sufficient to be converted under Conn. Gen. Stat. Ann. § 35-53(3). See Blue Cross & Blue Shield of Connecticut Inc. v. Carmen DiMartino (Conn. Super. Ct. 1991) available in LEXIS, States Library.

63. Del. Code Ann. § tit. 11, 935 (1991) (misuse of computer system information); id. § 933 (theft of computer services)

64. Ga. Code Ann. § 16-9-93(b) (1992) (the unlawful taking of computer programs or computer services is classified as computer trespass).

65. Ind. Code § 35-43-1-4 (Michie 1992) (computer tampering).

66. Ky. Rev. Stat. Ann. § 434.845(1) (Michie 1991) (unlawful computer access).

67. Me. Rev. Stat. Ann. § tit. 17, 432 (West 1992) (criminal invasion of computer privacy for unauthorized access).

68. Md. Code Ann., Crim. Law § 146 (1991) (illegal computer access)

69. Mich. Comp. Laws Ann. § 752.795(5) (West 1992) (fraudulent access to computers).

70. Nev. Rev. Stat. Ann. § 205.4765 (Michie 1991) (unauthorized copying of data or access to a computer is at least a misdemeanor)

71. N.J. Stat. Ann. § 2C:20-25(a) (West 1992) (criminal penalty for unauthorized taking of data from a computer); see also id. §§ 2C:20-25 to 20-29 (extensive provisions penalizing unauthorized copying or accessing of data).

72. N.Y. Penal Law § 156.25 (McKinney 1992) (crime of computer tampering only if data is altered or destroyed).

73. N.D. Cent. Code § 12.1-06.1-08(2) (Michie 1991) (unauthorized copying criminalized).

74. Tenn. Code Ann. § 39-14-602(b) (1992) (only punishes accessing computer systems, alteration and damage of data).

75. Tex. Penal Code Ann. § 33.02 (West 1992) (unauthorized access is a breach of computer security law). But see id. § 33.01(10) (copying of data is not included in the definition of damage.) For more information on these Texas laws, see Malcolm Uriah McClinchie III, Recent Development, Criminal Law Computer Crimes -- New Texas Penal Code Provision Establishing Criminal Penalties For Unauthorized Use and Tampering With Computers and Computer Data Bases. Tex. Penal code ann. §§ 33.01-.05 (Vernon supp. 1986), 17 St. Mary's L.J. 591 (1986).

76. See generally, Massachusetts Computer Crime Bill Proposed, 7 Computer Law. 45 (1990).

77. 18 U.S.C.S. § 1029 (Law. Coop. 1992). This law was the result of the Computer Fraud and Abuse Act of 1984 (CFAA); it was amended in 1986. See infra note 82 and accompanying text; see also Dodd S. Griffith, Note, The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem 43 Vand. L. Rev. 453 (1990) (and sources cited therein).

78. 18 U.S.C.S. § 1343 (Law. Coop. 1992).

79. 18 U.S.C.S. § 2512 (Law. Coop. 1992).

80. 42 U.S.C.S. § 2014(y) (Law. Coop. 1992) (the relevant codification of the Atomic Energy Act of 1954, codified throughout 2011-2296).

81. 18 U.S.C.S. § 2710 (Law. Coop. 1992). Section 2701 (dealing with unlawful access to stored communications) does not address computer worms or viruses. Computer Virus Hearings, supra note 1, at 39.

82. Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C.S. § 1030 (Law. Coop. 1992)). This provision was modified by a 1986 revision to include "federal interest" computers; see Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213. This provision is, currently, the primary statute addressing destructive computer program code such as viruses and worms. See Computer Virus Hearings, supra note 1, at 39.

83. Pub. L. No. 100-235, 101 Stat. 1724 (codified as amended in scattered sections of 18 & 40 U.S.C.) This Act divided responsibility for computer and data security between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). To comply with these provisions, the President enacted National Security Decision Directive (NSDD) 145. For an analysis of the relationship between the NSA and commercial computing activities, see Renae Angeroth Franks, Note, The National Security Agency and Its Interference with Private Sector Computer Security, 72 Iowa L. Rev. 1015 (1987) (analyzing NSDD 145 but acknowledging its withdrawal by the Reagan Administration); see also Statement on Signing the Computer Security Act of 1987, 24 Weekly Comp. Pres. Doc. 10 (Jan. 8, 1988).

84. See infra notes 151-53 and accompanying text (further discussing this legislative initiative).

85. 739 F. Supp. 414 (N.D. Ill. 1990) (memorandum order denying the majority of the defendants pretrial motions). The charges against Niedorf were later dropped. For an analysis of these events, see Current Developments, Motions to Dismiss Wire Fraud and Transport of Stolen Property Claims for Hacker Publishing Activity Denied But Charges Dropped, 7 Computer Law. 37 (1990). Riggs used a computer "bulletin board" to transfer the stolen software to Neidorf. For a general discussion of bulletin board legal issues, see generally, Jonathan Gilbert, Note, Computer Bulletin Board Operator Liability for User Misuse, 54 Fordham L. Rev. 439 (1988); Soma, Smith, & Sprague, Legal Analysis of Electronic Bulletin Board Activities, 7 W. New Eng. L. Rev. 571 (1985); Cheryl S. Massingale & A. Faye Borthick, Risk Allocation For Computer System Security Breaches: Potential Liability For Providers of Computer Services, 12 W. New Eng. L. Rev. 167 (1990).

86. Riggs and Niedorf, 739F. Supp. at 422.

87. Id.

88. 589 F.2d 152 (4th Cir.1978) (holding that programs are property).

89. This provision of the law states:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both.

18 U.S.C.A. § 1343 (West 1992). Further, the court held that the defendant had fraudulent intent in retrieving information from computer system without authorization. See Seidlitz, 589 F.2d at 160.

90. 507 F. Supp. 495 (E.D. Pa. 1981) (holding that computer time can be "stolen").

91. 488 F.2d 761 (8th Cir. 1973), cert. denied, 417 U.S. 909, and cert. denied, 417 U.S. 950 (1974).

92. Id. at 763-66 cited in Kelley, 507 F. Supp. at 499. The progeny of States has been uniform with the original holding. See United States v. Condolon, 600 F.2d 7, 8 (4th Cir. 1979); United States v. Louderman, 576 F.2d 1383, 1388 (9th Cir.), cert. denied, 439 U.S. 896 (1978); United States v. Brown, 540 F.2d 364, 374 (8th Cir. 1976).

93. Kelley, 507 F. Supp. at 499.

94. 446 F. Supp. 890 (D. Conn. 1978), aff'd, 601 F.2d 69 (2nd Cir. 1979) (holding that computer programs can be embezzled).

95. This statute punishes whoever

> embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted Shall be fined not more than $10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1,000 or imprisoned not more than one year, or both. The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

18 U.S.C.A. § 641 (West 1992). See infra notes 137-50 (discussing the Morison case).

96. Lambert, 446 F. Supp. at 892.

97. 365 F.2d 389 (2d Cir.), cert.denied, 385 U.S. 974 (1966).

98. 18 U.S.C.A. § 2314 (West 1992).

99. 365 F.2d at 393-94. The decision was cited approvingly in United States v. Robert J. Riggs and Craig Neidorf, 739 F. Supp. 414, 420 (N.D. Ill. 1990). See supra notes 85-87 and accompanying text (discussing Riggs).

100. 352 F. Supp. 915 (S.D.N.Y. 1972).

101. 18 U.S.C.A. § 2071 (West 1992) (punishing

> [w]hoever willfully and unlawfully conceals, removes, mutilates, obliterates, or destroys, or attempts to do so, or, with intent to do so takes and carries away any record, proceeding, map, book, paper, document, or other thing, filed or deposited with any clerk or officer of any court of the United States . . . .).

102. 538 F.2d 972 (3d Cir. 1976).

103. Id. at 978.

104. Id. at 978 n.10.

105. Lambert, 446 F. Supp. at 895.

106. Id.

107. 445 F.2d 1076 (9th Cir.), cert. denied sub nom., Jacobs v. United States, 404 U.S. 958 (1971) (upholding the conviction of a defendant charged with unauthorized photocopying and releasing of grand jury transcripts).

108. 402 S.W.2d 906 (Tex. Crim. App. 1966) (holding that programs are property).

109. Hancock, 402 S.W.2d at 908 (quoting the then applicable title 17, chapter 8, art. 1418 of the Texas Penal Code).

110. Id.

111. 418 So. 2d 847 (Ala. 1982) (holding that programs are property)

112. Ala. Code § 6-5-260 (1992). This code states that "[t]he owner of personalty is entitled to possession thereof. Any unlawful deprivation of or interference with such possession is a tort for which an action lies." Id. Section 6-5-260 does not address the issue of intangible personal property. See supra note 32 and accompanying text (describing Alabama's new law prescribing the taking of computer data).

113. See e.g. Latham v. State, 56 Ala. App. 234, 320 So. 2d 747 (1975); Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967); cf. State v. Central Computer Services Inc., 349 So. 2d 1160 (Ala. 1977) (holding that computer "software" was not tangible personal property for purposes of the state use tax but only because the statute involved applied explicitly to tangible personal property).

114. National Surety, 418 So.2d at 849.

115. Ala. Code § 13A-8-1(10) (1992) (the Alabama theft statute)

116. National Surety, 418 So. 2d at 850.

117. 459 N.E.2d 61 (Ind. Ct. App. 1984).

118. Id. at 62.

119. Theft is defined as where "[a] person who knowingly and intentionally exerts unauthorized control over property of another person with intent to deprive the other person of any part of its value or use, commits theft, a Class D felony." McGraw, 459 N.E.2 at 63 (quoting Ind. Code § 35-43-4-2(a)). Property

> means anything of value; and includes a gain or advantage or anything that might reasonably be regarded as such by the beneficiary; real property, personal property, money, labor, and services; intangibles; commercial instruments; written instruments concerning labor, services, or property; written instruments otherwise of value to the owner, such as a public record, deed, will, credit card, or letter of credit; a signature to a written instrument; extension of credit; trade secrets; contract rights, choses-in-action, and other interests in or claims to wealth; electricity, gas, oil, and water; captured or domestic animals, birds, and fish; food and drink; and human remains.

Id. (quoting Ind. Code § 35-41-1-2).

120. 151 Ind. App. 176, 278 N.E.2d 608 (1972) (holding that electricity, a service, may be stolen).

121. McGraw, 459 N.E.2d at 64. The McGraw court distinguished People v. Weg, 113 Misc. 2d 1017, 450 N.Y.S.2d 957 (1982), and Lund v. Commonwealth of Virginia, 217 Va. 688, 232 S.E.2d 745 (1977) (both reaching contrary conclusions) since both cases were based on more restrictive statutory interpretations. See infra notes 124-36 and accompanying text.

122. Id. at 64.

123. Id. This result is consistent with an analysis presented by Michael Gemignani, Computer Crime: The Law in the '80, 13 Ind. L. Rev. 681 (1980) (supporting the view of computer access as property).

124. 217 Va. 688, 232 S.E.2d 745 (1977) (holding computer time is not subject to theft).

125. Va. Code Ann. § 18.1(100) and 18.1(118) (Michie 1992).

126. Lund, 217 Va. at 690, 232 S.E.2d at 747.

127. Id.

128. Id. at 688, 232 S.E.2d at 746.

129. Id. at 692, 232S.E.2d at 748, citing Commonwealth v.McCray, 430 Pa. 130, 133, 242 A.2d 229, 230 (1968).

130. Id. quoting Va.Code Ann. § 18.1(100), 18.1(118).

131. Id. citing People v. Ashworth, 220 A.D. 498, 222 N.Y.S. 24, 27 (1927) (holding that the unauthorized use of machinery of another did not constitute larceny under New York's false pretense statute).

132. Lund, 217 Va. at 693, 232 S.E.2d at 749.

133. 450 N.Y.S.2d 957, 113 Misc. 2d 1017 (N.Y. Crim. Ct. 1982) (computer time is not subject to theft).

134. N.Y. Penal Law 165.15 (McKinney 1992). Subdivision 8 provides that a person is guilty of theft of services when

> [o]btaining or having control over labor in the employ of another person, or of **business, commercial or industrial** equipment or facilities of another person, knowing that he is not entitled to the use thereof, and with intent to derive a commercial or other substantial benefit for himself or a third person, he uses or diverts to the use of himself or a third person such labor, equipment or facilities.
>
> Id. (emphasis added).

135. Weg, 450 N.Y.S.2d at 960, 113 Misc. 2d at 1021 (presenting a detailed discussion of these three determinations).

136. See supra note 57 (citing the new Virginia Law), and supra note 72 (referring to New York's law that would penalize Weg but only if New York can prove that his activities altered or destroyed data).

137. 622 F. Supp. 1009 (1985), aff'd, 844 F.2d 1057 (4th Cir.), application denied, 486 U.S. 1306, cert. denied, 488 U.S. 908 (1988). Cf. United States v. Truong Dinh Hung, 629 F.2d 908, 923-28 (4th Cir. 1980) (Winter, J., separate concurrence) (opining that § 641 does not apply to theft of government information), and United States v. Tobias, 836 F.2d 449, 450-51 (9th Cir. 1988) (holding that § 641 does not apply to intangible property at all).

138. Morison, 844 F.2d at 1060.

139. Id. at 1061.

140. Id. at 1057. 18 U.S.C. § 793(d) and (e) relate to espionage. As these provisions do not relate to the issue of whether information is property, they will not be discussed further.

141. Morison, 844 F.2d at 1080.

142. Id. at 1076-77.

143. 484 U.S. 19 (1987).

144. Morison, 844 F.2d at 1077. The court however, stated that in the instant case there was no transfer of pure information but of actual government property. Id. Thus, its view of information as property may be deemed dicta but it is both revealing of the attitude of the Fourth Circuit and consistent with other circuits and with the Supreme Court. Cf. Dowling v. United States, 473 U.S. 207 (1985) (holding that 18 U.S.C. § 2314, relating to the interstate transportation of stolen goods, did not cover the conduct at issue in the case; the Court was looking for some physical taking of property).

145. 932 F.2d 306 (4th Cir. 1991).

146. 484 U.S. 19.

147. Id. at 25.

148. Fowler, 932 F.2d at 310. This view is consistent with leading scholars who also view information as property. See e.g. Raymond T. Nimmer & Patricia A. Krauthaus, Secured Financing and Information Property Rights, 2 High Tech. L.J. 195 (1987) (stating that "[i]nformation is an asset at the forefront of current technological development and commercial investment. It will remain there for the foreseeable future.").

149. Id. at 310 (also taking the opportunity to reaffirm Morison). The Fowler court was referring to United States v. Phillip Ray Jeter, 775 F.2d 670, 680-82 (6th Cir. 1985) (holding that grand jury transcripts are a "thing of value" under § 641), and United States v. George E. Girard Jr. and Paul A. Lambert, 601 F.2d 69, 70-71 (2d Cir. 1979) (holding that information can be converted under 18 U.S.C. § 641).

150. Morison, 844 F.2d at 1080.

151. See infra Annex I (presenting the current text of S. 1322).

152. Interview with Senate Judiciary Committee staff, in Washington, D.C. (Oct. 16, 1992).

153. S. 1322, proscribes, in part, activity by one who

> (5)(A) through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if-
>
> (i) the person causing the transmission intends that such transmission will-
>
> (I) damage, or cause damage to, a computer, computer system, network, information, data, or program or
>
> (II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program and
>
> (ii) the transmission of the harmful component of the program, information, code, or command-
>
> (I) occurred without the knowledge and authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command and
>
> (II) (aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period.

154. For a critical review of copyright protection of software, see Vance Franklin Brown, Comment, The Incompatibility of Copyright and Computer Software: An Economic Evaluation and a Proposal for a Marketplace Solution, 66 N.C. L. Rev. 977 (1988) (and sources cited therein).

155. See Software Piracy: SPA Hails Felonization Bill, 3:105 Edge, Oct. 19, 1992, available in LEXIS, Nexis Library, CURRNT File (Work-Group Computing Report). The Software Publishers Association is the principal trade association of the personal computer software industry. Its more than 950 members represent the leading publishers in the business, consumer and education software markets.

156. See Nintendo of America Applauds Passage of Copyright Felony Legislation, PR Newswire, Oct. 9, 1992, available in LEXIS, Nexis Library, CURRNT File.

157. See infra Annex II (presenting the text of S. 893).

158. See Software Piracy, supra note 155.

159. Id.

160. Id. (quoting the relevant testimony).

161. Id.

162. Id. (quoting the relevant testimony).

163. Id.

164. For further detail concerning S. 893, see 138 Cong. Rec. S17958 (daily ed. Oct. 8, 1992) (floor remarks of Senator Orrin Hatch).

165. Id.

166. Id. at S17959.

167. Council Directive 91/250 of 14 May 1991 on the Legal Protection of Computer Programs, 1991 O.J. (L 122) 42; see also infra Annex III (presenting the text of the directive in its entirety); Mike Lewis, What Software Copyright Laws Allow European Community's Directive on Software Copyright International Report Related to 'The High Cost of Software Piracy in Europe', 10:3 Data Based Advisor 130 (1992). For a discussion concerning a similar recent directive but concerning databases, see Jonathan Band & Laura F.H. McDonald, The Proposed EC Database Directive: The 'Reversal' of Feist v. Rural Telephone, 9 Computer Law. 19 (1992).

168. Alan Cane, Computer Groups Criticise Law, Fin. Times, Oct. 19, 1992, at 8.

169. Id.

170. The National Research Council (NRC) published a study entitled "Computers at Risk: Safe Computing in the Information Act." The study concludes that computer system breachers could cause economic disaster and even threaten human life. The NRC study declares that "[t]omorrow's terrorist may be able to do more damage with a keyboard than with a bomb." This study concludes that there is a need for an effective regime to protect computer systems. See 138 Cong. Rec. S17802-01, S17806 (daily ed. Oct. 8, 1992) (and sources cited therein).

171. See supra note 167 and accompanying text. A listing of EC countries showing their ratio of personal computer sales to sales of software packages (an important indicator of the level of software piracy) indicates a relationship between the intensity of copyright enforcement and the ratio, with a higher ratio indicating a lower incidence of piracy.

Nation(s)	Ratio	Level of Enforcement
United Kingdom	1.07	Strong
France	0.81	Moderate and increasing
Benelux	0.68	Weak
Germany	0.48	Moderate
Italy	0.33	Very weak, but improving
Spain	0.32	Weak

See Lewis, supra note 167. If software piracy were sharply curtailed, the software market would automatically double and 17,000 extra jobs would be created in the U.K. alone. See Sean Hallahan, Pirates Plundering Pounds 3bn a Year, The Times, July 3, 1992 available in LEXIS, Nexis Library, CURRNT File.

172. The position of the United States Justice Department is that a conversion is not necessary to convict under § 641. A recent court decision noted, however, that not every violation of § 641 requires a conversion but did not expressly rule upon this position. See United States v. Bernie E. Zettl, 889 F.2d 51 (4th Cir. 1989). This position by the Justice Department, not discouraged by the Fourth Circuit, means that damage caused by the taking of a thing of value does not require a conversion of property under § 641.

173. 739 F.414 Ill. pl324 (1991) See note 85-87 and accompanying text.

174. 589 F.2d 152 (4th Cir. 1978). See supra notes 88-89 and accompanying text.

175. 507 F. Supp.495(E.D.Pa. 1981). See supra note 90 and accompanying text.

176. 446 F. Supp. 890 (D. Conn. 1978). See supra notes 94-96 and accompanying text.

177. 402 S.W.2d 906 (Tex. Crim. App. 1966). See supra notes108-10 and accompanying text.

178. 418 So. 2d 847 (Ala.1982). See supra notes 111-16 and accompanying text.

179. 459 N.E.2d 61 (Ind. Ct. App. 1984). See supra notes 117-23 and accompanying text.

180. 844 F.2d 1057 (4th Cir. 1988). See supra notes 137-50. Morison is also consistent with a similar holding in United States v. Girard, 601 F.2d 69 (2d Cir.), cert. denied, 444 U.S. 871 (1979).

181. 484 U.S. 19 (1987) See supra notes 143-47 and accompanying text.

182. 932 F.2d 306 (4th Cir. 1991). See supra notes 145-49 and accompanying text.

183. For an analysis of the extent of enforcement and remedies available under trade secret laws, see Donald M. Zupanec, Annotation, Criminal Liability for Misappropriation of Trade Secrets, 84 A.L.R.3d 967 (1992). For general information concerning trade secret law in a computer software context, see generally, Robert C. Scheinfeld & Gary M. Butter, Using Trade Secret Law to Protect Computer Software, 17 Rutgers Computer & Tech. L.J. 381 (1991); John C. Yates & Michael W. Mattox, Intellectual Property, 42 Mercer L. Rev. 295 (1990); Edward M. Kalinka, Jeffery M. Brinza & Gregory J. Parry, Protecting Software in the Sale of Equipment From Reverse Engineering, Mich. B.J. 564 (1990); Ronald Abramson, Trade Secret Protection For Computer Software -- Procedures For Protection: Recent Decisions on its Scope (1990) (PLI Order No. G4-38S4); Michael J. McNeil, Trade Secret Protection For Mass Market Computer Software: Old Solutions For New Problems, 51 Alb. L. Rev. 293 (1987); David Bender, Protecting Computer Trade Secrets (1986) (PLI Order No. G4-3790); Douglas K. Southard, Trade Secrets and the Criminal Law: A View From 'Silicon Valley' (1986) (PLI Order No. G4-3790); Cynthia M. York, Note, Criminal Liability for the Misappropriation of Computer Software Trade Secrets, 63 U. Det. L. Rev. 481 (1986); Vitauts M. Gulbis, Disclosure or Use of Computer Application Software as Appropriation of Trade Secret, 30 A.L.R.4th 1250 (and sources cited therein); Donald M. Zupanec, Criminal Liability for Misappropriation of Trade Secret, 84 A.L.R.3d 967 (1992); Page M. Kaufman, Note, The Enforceability of State "Shrink-Wrap" License Statutes in Light of Vault Corp. v. Quaid Software Ltd., 74 Cornell L. Rev. 222, 230 n.60 (1988); Susan C. Miller, Review of Florida Legislation Comment: Florida's Uniform Trade Secrets Act, 16 Fla. St. U. L. Rev. 863, 867 n.25 (1988); Beverly D. Horn, Protecting Trade Secrets in the Information Age, 4 JAN Nat. Resources & Env't 22 (1990); and Victoria A. Cundiff, Thinking About Trade Secrets: How to Identify and Maintain Your Competitive Advantage (1992) (PLI Order No. G4-3884).

184. U.S. Const., art. I, § 8, cl. 3. A Federal Trade Secrets Act already exists but it is not modeled on state laws. See 18 U.S.C.A. § 1905 (West 1992). It prohibits only U.S. Government employees from revealing trade secret information provided to regulators. See Elinor P. Schroeder & Sidney A. Shapiro, Responses to Occupational Disease: The Role of Markets Regulation and Information, 72 Geo. L.J. 1231, 1282 n.444 (1984). The need for a new Federal Trade Secrets law has long been documented. See, e.g. Pamela Samuelson, The Semiconductor Chip Protection Act of 1984 and its Lessons: Creating a New Kind of Intellectual Property: Applying the Lessons of the Chip Law to Computer Programs, 70 Minn. L. Rev. 471, 519 (1985) (and sources cited therein); Southard, Trade Secrets and the Criminal Law, supra note 183; Michael B. Einschlag & Peter L. Michaelson, Patent and Trade Secret Protection of Software: Patentability of Programs--Nature and Scope of Trade Secret Protection (1986) (PLI Order No. G4-3791).

185. See Restatement of the Law of Torts, § 757 (1967) (along with Comment (b) presenting a generally accepted definition of trade secret). Just what can be considered a trade secret is a very broad category, but it does not include all "know how." See Mycalex Corp. of America v. Pemco Corp., 64 F. Supp. 420, aff'd 159 F.2d 907 (4th Cir. 1947); see also United States v. Timken Roller Bearing Co., 83 F. Supp. 284 (N.D. Ohio 1949).

186. See Restatement of the Law of Torts, supra, § 757 (and comments therein).

187. See United States v. Aluminum Co. of America (Alcoa), 148 F.2d 416, 443 (2d Cir. 1945) (sitting by designation as the Supreme Court lacked a quorum) (adopting an expansive formulation of extra-territorial application of U.S. antitrust laws with jurisdiction based on a twin-pronged test which considers effects upon the United States); see also Industrial Investment Development Corp. v. Mitsui Co., 67 F.2d 876 (5th Cir. 1982) (refusing to dismiss an antitrust suit merely because the parties were foreign and all relevant actions took place outside the United States); see also Restatement (Third) Foreign Relations Law of the United States §§ 402-03, 416 (1987) (discussing extraterritorial jurisdiction); U.S. Department of Justice, Antitrust Enforcement Guidelines for International Operations 104 (1988) (acknowledging the extra-territorial application of selected antitrust doctrines). Cf. Timberlane Lumber Co. v. Bank of America N.T. & S.A., 749 F.2d 1378 (9th Cir. 1984) (also known as Timberlane II) (applying a new tripartite analysis which would not be hostile to a future Federal trade secrets law).

188. The U.S. security laws have frequently been applied to conduct occurring abroad. See e.g., Psimenos v. E. F. Hutton & Co., 722 F.2d 1041 (2d Cir. 1983); see also Gary B. Born & David Westin, International Civil Litigation in United States Courts: Commentary & Materials 474 n.114 (1991) (and sources cited therein). U.S. courts have

"consistently applied the federal commodities and securities laws extraterritorially." Id. at 480.

189. Those firms who seek Federal protection of their industrial secrets purposely avail themselves of the U.S. judicial system and may reasonably find themselves subject to U.S. jurisdiction regardless of the actual location of other divisions or official personnel of the relevant parent firm of the targeted U.S. technology or defense firm. See, e.g., WorldWide Volkswagen v. Woodson, 444 U.S. 286 (1980), Afram Export Corp. v. Metallurgiki Halyps, S.A., 772 F.2d 1358 (7th Cir. 1985), Asahi Metal Industry Co. v. Superior Court of California, Solano County, 107 S. Ct. 1026 (1987).

190. See, e.g., Burger King v. Rudzewicz, 471 U.S. 462 (1985) (affirming jurisdiction on, inter alia, grounds that mere commercial contracts provides a reasonable basis on which to base jurisdiction for an out-of-state business relation).

191. See, e.g., The Bremen v. Zapata Off-Shore Co., 407 U.S. 1 (1972)

192. See, e.g., Mistubishi Motors Corp. v. Soler ChryslerPlymouth, Inc., 473 U.S. 614, 637 n.21 (1985).

193. See, e.g., id. (generally supporting the policies behind international commercial arbitration and enforcement of arbitral decisions).

194. 50 U.S.C. §§ 2401-13 (1988) (together with the Arms Export Control Act, discussed immediately infra, requires validated licenses to export specified categories of technology, arms, and other goods to foreign buyers).

195. 22 U.S.C. § 2778 (1988); see also supra (discussing the joint purpose of this act and the Export Administration Act); 22 C.F.R. § 120.1-.25 (1992) (regulating the international traffic in arms).

196. See 32 C.F.R. § 2-201(a) (1992). These regulations are issued under the authority of the National Security Act of 1947. See 50 U.S.C. § 401 (1986).

197. 50 U.S.C. § 1 (1988) (making it illegal to engage in any form of trade with an enemy or an ally of an enemy of the United States during wartime, subject to specified exceptions).

198. This concern is echoed by the Computer and Business Equipment Manufacturers Association (CBEMA), an industry trade group. See Computer Virus Hearings, supra note 1, 94 (stating that "[t]he same technology that can introduce a harmful virus into all the files in a computer system, can also be used for the beneficial purpose of finding and eliminating problems.").

APPENDIX

Annex I: Senate Bill 1322

Title XXVII - Computer crime

SEC. 404. COMPUTER ABUSE AMENDMENTS ACT OF 1992.

(a) SHORT TITLE.
-This section may be cited as the "Computer Abuse Amendments Act of 1992."

(b) PROHIBITION.
-Section 1030(a)(5) of title 18, United States Code, is amended to read as follows:

"(5)(A) through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if

"(i) the person causing the transmission intends that such transmission will-

"(I) damage, or cause damage to, a computer, computer system, network, information, data, or program or

"(II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program and

"(ii) the transmission of the harmful component of the program, information, code, or command-

"(I) occurred without the knowledge and authorization of the persons or entitites who own or are responsible for the computer system receiving the program, information, code, or command and

"(II) (aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period or

"(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals or

"(B) through means of a computer used in interstate commerce or communication, knowingly causes the transmission of a program, information, code, or command to a computer or computer system-

"(i) with reckless disregard of a substantial and unjustifiable risk that thetransmission will-

"(I) damage, or cause damage to, a computer, computer system, network,information, data or program or

"(II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data or program and

"(ii) if the transmission of the harmful component of the program, information, code, or command-

"(I) occurred without the knowledge and authorization of the persons orentities who own or are responsible for the computer system receiving the program, information, code, or command and

"(II) (aa) causes loss or damage to one or more other persons of a value aggregating $1,000 or more during any 1-year period or

"(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals."

(2) PENALTY.-Section 1030(c) of title 18, United States Code. is amended-

(A) in paragraph (2)(B) by striking "and" after the semicolon

(B) in paragraph (3)(A) by inserting "(A)" after "(a)(5)"

(C) in paragraph (3)(B) by striking the period at the end thereof and inserting ", and" and

(D) by adding at the end thereof the following:

"(4) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B)."

(3) CIVIL ACTION.
-Section 1030 of title 18, United States Code, is amended by adding at the end thereof the following new subsection:

"(g) Any person who suffers damage of loss by reason of a violation of the section, other than a violation of subsection (a)(5)(B), may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.".

(4) REPORTING REQUIREMENTS.
-Section 1030 of title 18, United States Code, is amended by adding at the end thereof the following new subsection:

"(h) The attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under section 1030(a)(5) of title 18, United States Code.".

(5) PROHIBITION.
-Section 1030(a)(3) of title 18, United States Code, is amended by inserting "adversely" before "affects the use of the Government's operation of such computer."

Annex II: Senate Bill 893

Date of Introduction: October 8, 1992
Date of Version: October 17, 1992 (Version: 7)

An Act

To amend title 18, United States Code, with respect to the criminal penalties for copyright infringement.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. CRIMINAL PENALTIES FOR COPYRIGHT INFRINGEMENT.

Section 231 ɔ) of title 18, United States Code, is amended to read as follows:

"(b) Any person who commits an offense under subsection (a) of this section-

"(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title,or both, if the offense consists of the reproduction or distribution, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, with a retail value of more than $2,500

"(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1) and

"(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.".

SECTION 2. CONFORMING AMENDMENTS.

Section 2319(c) of title 18, United States Code, is amended-

(1) in paragraph (1) by striking "'sound recording', 'motion picture', 'audiovisual work', 'phonorecord'," and inserting "'phonorecord "' and

(2) in paragraph (2) by striking "118" and inserting "120"

Annex III: EC Directive on Software Protection

Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC) the Council of the European Communities, having regard to the treaty establishing the European Economic Community and in particular article 100a thereof, having regard to the proposal from the Commission

(1), in cooperation with the European Parliament

(2), having regard to the opinion of the economic and social committee

(3), whereas computer programs are at present not clearly protected in all member states by existing legislation and such protection, where it exists, has different attributes;

whereas the development of computer programs requires the investment of considerable human, technical and financial resources while computer programs can be copied at a fraction of the cost needed to develop them independently;

whereas computer programs are playing an increasingly important role in a broad range of industries and computer program technology can accordingly be considered as being of fundamental importance for the community's industrial development;

whereas certain differences in the legal protection of computer programs offered by the laws of the member states have direct and negative effects on the functioning of the common market as regards computer programs and such differences could well become greater as member states introduce new legislation on this subject;

whereas existing differences having such effects need to be removed and new ones prevented from arising, while differences not adversely affecting the functioning of the common market to a substantial degree need not be removed or prevented from arising;

whereas the community's legal framework on the protection of computer programs can accordingly in the first instance be limited to establishing that member states should accord protection to computer programs under copyright law as literary works and, further, to establishing who and what should be protected, the exclusive rights on which protected persons should be able to rely in order to authorize or prohibit certain acts and for how long the protection should apply;

whereas, for the purpose of this directive, the term 'computer program' shall include programs in any form, including those which are incorporated into hardware;

whereas this term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage;

whereas, in respect of the criteria to be applied in determining whether or not a computer program is an original work, no tests as to the qualitative or aesthetic merits of the program should be applied; whereas the community is fully committed to the promotion of international standardization;

whereas the function of a computer program is to communicate and work together with other components of a computer system and with users and, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function;

whereas the parts of the program which provide for such interconnection and interaction between elements of software and hardware are generally known as 'interfaces'; whereas this functional interconnection and interaction is generally known as 'interoperability';

whereas the exclusive rights of the author to prevent the unauthorized reproduction of his work have to be subject to a limited exception in the case of a computer program to allow the reproduction technically necessary for the use of that program by the lawful acquirer;

whereas this means that the acts of loading and running necessary for the use of a copy of a program which has been lawfully acquired, and the act of correction of its errors, May not be prohibited by contract;

whereas, in the absence of specific contractual provisions, including when a copy of the program has been sold, any other act necessary for the use of the copy of a program May be performed in accordance with its intended purpose by a lawful acquirer of that copy;

whereas a person having a right to use a computer program should not be prevented from performing acts necessary to observe, study or test the functioning of the program, provided that these acts do not infringe the copyright in the program;

whereas the unauthorized reproduction, translation, adaptation or transformation of the form of the code in which a copy of a computer program has been made available constitutes an infringement of the exclusive rights of the author;

whereas, nevertheless, circumstances May exist when such a reproduction of the code and translation of its form within the meaning of article 4 (a) and (b) are indispensable to obtain the necessary information to achieve the interoperability of an independently created program with other programs;

whereas it has therefore to be considered that in these limited circumstances only, performance of the acts of reproduction and translation by or on behalf of a person having a right to use a copy of the program is legitimate and compatible with fair practice and must therefore be deemed not to require the authorization of the rightholder;

whereas an objective of this exception is to make it possible to connect all components of a computer system, including those of different manufacturers, so that they can work together;

whereas such an exception to the author's exclusive rights May not be used in a way which prejudices the legitimate interests of the rightholder or which conflicts with a normal exploitation of the program;

whereas, in order to remain in accordance with the provisions of the Berne convention for the protection of literary and artistic works, the term of protection should be the life of the author and fifty years from the first of January of the year following the year of his death or, in the case of an anonymous or pseudonymous work, 50 years from the first of January of the year following the year in which the work is first published;

whereas protection of computer programs under copyright laws should be without prejudice to the application, in appropriate cases, of other forms of protection;

whereas, however, any contractual provisions contrary to article 6 or to the exceptions provided for in article 5 (2) and (3) should be null and void;

whereas the provisions of this directive are without prejudice to the application of the competition rules under articles 85 and 86 of the treaty if a dominant supplier refuses to make information available which is necessary for interoperability as defined in this directive;

whereas the provisions of this directive should be without prejudice to specific requirements of community law already enacted in respect of the publication of interfaces in the telecommunications sector or Council decisions relating to standardization in the field of information technology and telecommunication;

whereas this directive does not affect derogations provided for under national legislation in accordance with the Berne convention on points not covered by this directive, has adopted this directive:

Article 1 object of protection

1. In accordance with the provisions of this directive, member states shall protect computer programs, by copyright, as literary works within the meaning of the Berne convention for the protection of literary and artistic works. For the purposes of this directive, the term 'computer programs' shall include their preparatory design material.
2. Protection in accordance with this directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this directive.
3. A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.

Article 2 authorship of computer programs

1. The author of a computer program shall be the natural person or group of natural persons who has created the program or, where the legislation of the member state permits, the legal person designated

as the rightholder by that legislation. Where collective works are recognized by the legislation of a member state, the person considered by the legislation of the member state to have created the work shall be deemed to be its author.
2. In respect of a computer program created by a group of natural persons jointly, the exclusive rights shall be owned jointly.
3. Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract.

Article 3 beneficiaries of protection shall be granted to all natural or legal persons eligible under national copyright legislation as applied to literary works.

Article 4 restricted acts subject to the provisions of articles 5 and 6, the exclusive rights of the rightholder within the meaning of article 2, shall include the right to do or to authorize:
(a) the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole. Insofar as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorization by the rightholder;
(b) the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program; (c) any form of distribution to the public, including the rental, of the original computer program or of copies thereof. The first sale in the community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the community of that copy, with the exception of the right to control further rental of the program or a copy thereof.

Article 5 exceptions to the restricted acts
1. In the absence of specific contractual provisions, the acts referred to in article 4 (a) and (b) shall not require authorization by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.
2. The making of a back-up copy by a person having a right to use the computer program May not be prevented by contract insofar as it is necessary for that use
3. The person having a right to use a copy of a computer program shall be entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.

Article 6 decompilation
1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:
(a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to so;

(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and
(c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.
2. The provisions of paragraph 1 shall not permit the information obtained through its application:
(a) to be used for goals other than to achieve the interoperability of the independently created computer program;
(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or
(c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.
3. In accordance with the provisions of the Berne convention for the protection of literary and artistic works, the provisions of this article May not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the right holder's legitimate interests or conflicts with a normal exploitation of the computer program.

Article 7 special measures of protection
1. Without prejudice to the provisions of articles 4, 5 and 6, member states shall provide, in accordance with their national legislation, appropriate remedies against a person committing any of the acts listed in subparagraphs (a), (b) and (c) below:
(a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;
(b) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;
(c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which May have been applied to protect a computer program.
2. Any infringing copy of a computer program shall be liable to seizure in accordance with the legislation of the member state concerned.
3. Member states May provide for the seizure of any means referred to in paragraph 1 (c).

Article 8 term of protection
1. Protection shall be granted for the life of the author and for fifty years after his death or after the death of the last surviving author; where the computer program is an anonymous or pseudonymous work, or where a legal person is designated as the author by national legislation in accordance with article 2 (1), the term of protection shall be fifty years from the time that the computer program is first lawfully made available to the public. The term of protection shall be deemed to begin on the first of January of the year following the above mentioned events.
2. member states which already have a term of protection longer than that provided for in paragraph 1 are allowed to maintain their present term until such time as the term of protection for copyright works is harmonized by community law in a more general way.

Article 9 continued application of other legal provisions

1. The provisions of this directive shall be without prejudice to any other legal provisions such as those concerning patent rights, trade-marks, unfair competition, trade secrets, protection of semi-conductor products or the law of contract. Any contractual provisions contrary to article 6 or to the exceptions provided for in article 5 (2) and (3) shall be null and void.
2. The provisions of this directive shall apply also to programs created before 1 January 1993 without prejudice to any acts concluded and rights acquired before that date.

Article 10 final provisions

1. Member states shall bring into force the laws, regulations and administrative provisions necessary to comply with this directive before 1 January 1993. When member states adopt these measures, the latter shall contain a reference to this directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such a reference shall be laid down by the member states.
2. Member states shall communicate to the Commission the provisions of national law which they adopt in the field governed by this directive.

Article 11 this directive is addressed to the member states. Done at Brussels, 14 May 1991.

Defining the Threat to Information Systems: A Challenge for Security Educators

Lynn F. Fischer
Department of Defense Security Institute

The common use of automated information systems components in the modern workplace in both government and industry and the need to protect information from competing interests at both the national and corporate level has necessitated (1) the application of security countermeasures appropriate to automated systems, and (2) additional security education for personnel having access to these systems. The implementation of both these activities presumes the existence of a persistent "threat" from external sources--a threat, although taken for granted, which often lacks clear definition in terms of (a) what exactly is being threatened, (b) why it is being threatened, (c) where is the threat coming from, (d) how might it be carried out, (e) and what are we supposed to be doing to prevent it?

These are actually the classic questions faced by security educators everywhere, in automated and non-automated environments alike. And the historic objectives of security awareness programs in government aimed at the protection of classified and sensitive information is to provide credible answers to these questions, thus providing employees with the knowledge and motivation to prevent protected information from falling into the wrong hands. In fact, for the government security educator, never has the need to define a credible external threat been so urgent as now, following the collapse of the Soviet Empire and the dismemberment of communist regimes. We are constantly challenged by cleared personnel to explain why, since the KGB is no more, we need an array of elaborate protective measures.

Developing a Strategy for Security Awareness

Therefore the central purpose of this monograph is to map out what might be an appropriate educational strategy for a security educator confronted with the new challenge of giving a "computer security briefing" or, more properly stated, educating employees in information systems security. Before attempting to do this, I must spell out several assumptions that will impact on the professional life of the persons assigned this responsibility.

One of these is that we must assume that educational activities related to information systems security in the future will be carried out by a *generalist* security professional who does not have special qualifications in automated information systems, computer science, or electrical engineering. Just as the medium of paper is a given, so it is that in the modern workplace, the use of electronic media and processing is assumed.

Another, closely related proposition is that the conceptual distinction between conventional information security and "information systems security" is artificial. At least it has been a

convenient way to organize the work of security professionals. At its worst, it perpetuates the myth that security countermeasures in an automated environment is too technical for just anybody to understand.

And third, information security in any type of environment is essentially a human issue. In simple terms, we can spend millions on NSA endorsed "trusted systems," but if the people who have access to those systems are not trust-worthy (loyal, reliable, competent and aware) it's all for nothing.

Perhaps the most difficult aspect of this challenge to the security specialist in government or facility security officer in industry who is tasked with security education is how to approach the job: what is important to include (and not to include) in an educational program, and how to organize that material. What follows is, in my opinion, some good advice about the central arguments that we need to get across to an often times skeptical audience.

By no means are these ideas all original with me. In fact, my thinking has been greatly influenced by experienced security educators such as Joseph Grau at the Department of Defense Security Institute, and more recently by Captain John McCumber of the Defense Information Systems Agency who has written extensively on informations systems security. In addition, I would like to propose that much of what has been good advice to security educators for years in non-automated environments is still good advice. However, the same principles may have to be described with new terminology, and remedies prescribed as new and somewhat different countermeasures.

Beginning with Objectives

Undoubtedly the most useful advice I have been given by professional trainers, and in turn have promoted, is that effective security education begins with clear objectives. In developing a communications program to a target audience we should be asking ourselves the question: "What are my goals, performance objectives, or principal arguments of this briefing, newsletter, video product, or other educational event?" Rather than deal with performance objectives in the formal sense here, I would only attempt to identify a set of propositions or arguments that the educators would want to support and establish in the minds of a target audience:

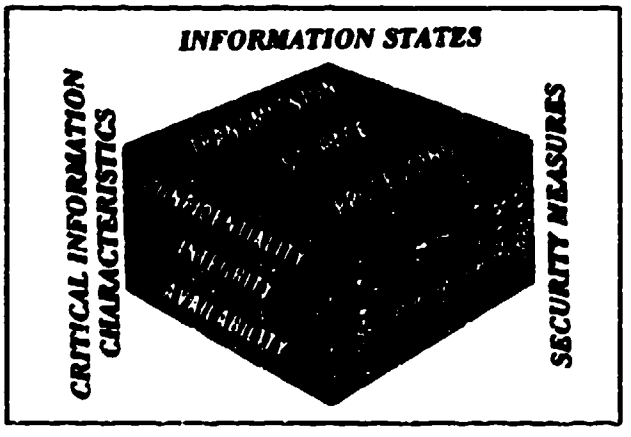
1. "Information systems security" is no more than information security for the modern workplace. We are building on long-established principles, policies, and practices.

Not everybody in the security profession is happy about this idea. At the most recent Department of Defense Security Conference heated and anguished objections were raised by many senior security officers about discussing AIS/computer security as "Infosec." However we

may slice up the policy or distribute the procedural duties in the security world, the fact remains that the above proposition can make sense to the rank and file employees if properly explained. Furthermore, if we can successfully sell the idea, this will go a long way to demythicize security countermeasures for automated systems and electronic processing. And as a result, our personnel will begin to see information systems security as a human issue rather than as a technical problem.

McCumber's Three-dimensional Infosec Model

How can we achieve this educational objective? There are no easy answers, but of particular value not only for organizing our own thinking but possibly as an instructional device itself, is John McCumber's Infosec Model seen below:



Using the above three-dimensional diagram, McCumber tells us that information in any of three states (transmission, storage, or processing) is subject to three types of threat (to its confidentiality, integrity, and its availability to a legitimate user). The threat, if realized, would be carried out by a perpetrator through theft, corruption, and destruction or denial of access. McCumber's third dimension categorizes security countermeasures appropriate for each state and each critical characteristic. Again the measures or countermeasures are of three types: technology, policy & practice, and education. What we end up with is a three-dimensional map for evaluating the security effectiveness of any given information system. Theoretically, the resulting 27 cells can be evaluated independently, each with its own appropriate security countermeasures.

While intelligible and useful to an analyst perhaps engaged in system certification (which apparently was McCumber's original intent), one should hesitate to employ this model as an instructional aid to a typical audience or readership. At first glance, it is not user-friendly and

it is somewhat at odds with the best advice of more seasoned trainers: KISS or "keep it simple stupid" or you lose your audience. But there are simpler variations of this model that have potential for security education. One is seen in McCumber's article in the *Security Awareness Bulletin* (September 1991) in which countermeasures falling into three categories are identified for each of three states of information. This in my opinion does have potential as a way to get people thinking about how we protect information in an automated environment.

Layers of Security Measures by Information States

	TRANSMISSION	STORAGE	PROCESSING
TECHNOLOGY	STU-III Data encryption devices Code Parity error checks	Access codes Password controls Physical safeguards Intrusion protection SCIF construction	Trusted systems (NSA) User recognition systems Multi-level processing Error traps Anti-virus software
POLICY/ PRACTICE	Data encryption standards Personnel security	User access policy User authorization Approved systems (DIS) Physical safeguards Approved storage Personnel security	Access control policy Approved systems (DIS) Audit trails Personnel security
EDUCATION TRAINING AWARENESS	COMSEC training STU-III indoctrination	Security indoctrination Physical protection training	Security indoctrination Security education Computer security briefings

But more importantly, this framework provides the opportunity for comparing security countermeasures of all types including the traditional world of paper, padlocks, inkpads and file cabinets. Actually only a few of the total inventory of security countermeasures for the workplace are listed above. It might be possible, as an interesting instructional exercise to identify comparable measures for a non-automated environment for each measure appropriate for information systems security.

Probably the logical conclusion to this exercise would be to reaffirm the basic principles of information security such as need-to-know, accountability, control of access, physical protection, personal safeguarding, and employee responsibility for reporting. As new technologies for the transmission, storage and processing of information emerge, we simply add new and technologically appropriate countermeasures to the inventory.

2. Severe damage to government and defense-related information by both internal and external offenders has occurred in the very recent past. It can happen to any organization, and the damage can be significant.

Appended to this paper is a rough attempt to list the more important criminal cases or events which have affected defense-related information systems since 1987. Included here are only those events which have come to public knowledge through media coverage. Also seen here are a few cryptic notes on systems penetrated, damage or compromise, and possible motivations. Behind each entry is an interesting case study in itself. Most, but not all, of these events are related to computer hacking--defined in the 1990s as illegal or unauthorized access to a system or network using telephonic communication from a remote site.

The use of this case study information in security education is a long and honored tradition which most of us believe is extremely effective if handled correctly. We have seen in the past that one of the best ways to capture the attention of an audience is to tell them stories, particularly stories about the sins and failings of people just like themselves. Perhaps for the same reason people love soap operas--nevertheless, these stories work and they serve as vehicles for several teaching objectives.

The discussion of classic espionage cases in security awareness briefings and video products brings the foreign intelligence threat and the act of espionage into the world of reality. In video format, seeing the face of a convicted spy--who may look no more unusual than the person in the next cubicle--leads the viewer to understand that it can happen *here*. Furthermore, by showing the extensive damage to national security resulting from each betrayal, our employees are (we hope) more willing to see security countermeasures as being important and worth implementing since they may even save lives.

Thus by adopting the strategy of a traditional security educator who wants to make "the threat" credible, and by a regular exploitation of media sources and unclassified reports, we can put a human face on computer crime. We can discuss, for example, the type of people who might attempt to sabotage a system with a Trojan horse or virus. We can get an idea about what motivates some teenagers to create havoc in some of the most extensive research networks in the nation.

As in the classic espionage cases, each of these computer crime stories offers lessons learned. However, one big difference between the two categories of events is that in almost all of the recent classic espionage cases--John Walker, Thomas Cavanagh, William Bell, James Hall, Larry Wu Tai Chin--betrayal of public trust is a common denominator. However, this is much less typical of computer crime cases endangering national security where the perpetrator was never authorized access to the system into which he intruded.

There are two or three inside-jobs listed here, but in most of these events the crime is "breaking and entering" by a total outsider.

3. Foreign intelligence services represent only one of several sources of threat to our systems. We have to address both external and internal threats.

Referring again to one of the eternal questions that each security educator is duty bound to answer: "Where is the threat coming from?" we can see here a contrast between classic espionage and contemporary computer crime. Whereas the former events nearly always involve foreign interests and foreign intelligence services at some point in the activity, computer crime endangering national security rarely is associated with a foreign intelligence organization among the cases that are openly acknowledged. But this may be illusory; it is quite conceivable that the penetration of sensitive government and defense contractor systems by foreign intelligence services is routinely so successful that it goes unnoticed or is not openly acknowledged.

In 1986 press reports announced the probable exploitation of unclassified but sensitive U.S. defense-related data through a Vienna-based research institute which employed both Western and Soviet Bloc scientists. This was done by conventional long-distance telephone and with legitimate access procedures.

The only publicly admitted instance of foreign intelligence involvement in a hacking scheme was seen in the case of the West German Hackers who served as a conduit for sensitive U.S. Government information going to the KGB. The full account of this story is found in Clifford Stoll's entertaining book, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. The case of Michael Peri, who physically delivered classified floppy disks and a computer with a classified file on the hard drive to East German Intelligence — a unique event. Of the other offenders listed here, only Kevin Lee Poulsen was charged under the espionage code for having illegally obtained a classified document (presumably by electronic transmission). This was reported to have been an Air Force Tasking Order, containing flight orders for Army paratroopers on a 1987 military exercise at Fort Bragg, N.C.

In most of the events that concern the penetration of a national-level information system, what we do see reported, however, is an act committed not by a representative of foreign interests but by a very young individual whose motives are not clear and who may have no real interest in providing illegally accessed information to any foreign interest. In many of these situations it turned out that the greatest threat to the information posed by hackers was not so much in its being compromised, but in its being altered, destroyed, or denied to legitimate users.

One can note in the examples cited here the predominance of a "domestic" threat; and in many cases of computer crime in which private sector systems and data are targeted for illegal profit (not included in the listing which follows), the culprit is typically an "insider;" that is, a person like logic bomber Michael Lauffenberger who had authorized access to the system, if not to all of the information contained in that system. These are some of the significant differences and similarities between what might be called the conventional threat to protected information and the emerging threat to information systems.

Motivation: Why do they do it?

While independent organizations such as the American Society for Industrial Security report annually on the enormous cost to private sector firms from computer crime apparently committed for financial gain, those who attack and penetrate national-level and defense community systems may be driven by far more complex motives. At this point in time, suggestions about the underlying motivations of Herbert Zinn, the Legion of Doom, the Dutch or Australian Hackers, Kevin Poulsen and others is conjecture. However, press reports mention such things as intellectual challenge, thrill, ego satisfaction, a craving for recognition and prestige, and boosting self-esteem as driving forces. The *New York Times* quoted one unnamed researcher at a Silicon Valley research institution as concluding that these hackers have an anti-social obsession. In recent years, the article states, the researcher offered four underground hackers programming jobs in an effort to channel their energy away from the destructive use of computers. In each case the experiment failed:

> "They're misfits, losers or troubled individuals lacking a sense of duty or morals. ...Every single one of them had deep psychological problems." (Markoff, 1988)

Fortunately, to better address this issue, the Community Research Center, a group of Federal agency clinical psychologists, has initiated work on the psychological make-up of computer offenders. This, like CRC's ongoing study of espionage felons (Project Slammer), will be based on in-depth interviews with each offender.

What can be said to our employee populations about the reality of the external threat?

With the help of counterintelligence professionals in the FBI, DIA and other agencies, we are beginning to articulate a response to this challenge that is both believable to our employee populations and factually accurate. Without going into unnecessary detail the arguments are these: While the KGB in name is gone, the GRU remains active and the post-soviet Russians still target critical defense-related information. The foreign intelligence threat is coming at us from diverse sources--friend and foe alike. This includes

organizational entities which are not nation-states: international corporations, terrorist groups, rebel factions, and organized crime. High on the list of targeted information is advanced technology having military application which may or may not be formally classified. Lastly we know that our economic competitors overseas work very closely with their respective national intelligence organizations to acquire our protected technologies. And there is no reason to believe that these intelligence services have failed to take advantage of human talents and new technologies that can be mobilized to penetrate our information systems.

This recent redefinition of the foreign intelligence threat for the 1990s and beyond is relevant to the issue of information systems security since it broadens the range of possible non-domestic sources about which we must be alert. But for the security educator who is tasked with the job of briefing and in other ways educating co-workers, supervisors, and executives functioning in an automated workplace, this is only part of the answer, and as discussed above, the source of the threat is only one of the several awareness issues that must be addressed.

4. We are not helpless when confronting these potential threats to automated systems. There are things that every employee can do to minimize the risk of compromise or loss of information.

This is always one of the themes (or should be) of an effective security awareness communication to employee populations whose members have the responsibility for safeguarding classified or sensitive information. Having informed people of the reality of a threat, we then need to tell them what they can do about it. Regrettably some security educators don't construct for their audiences the link between the threat to information and the application of specific security countermeasures. Another frequently missing element in security education is specific information about past damage from security failures and potential consequences of future disasters. All the more reason to review past crime and espionage cases where the damage can be spelled out in dollars or military consequences.

We are told that our employees *will* pay attention to security briefings if they are provided with specific information that is concretely related to their day-to-day tasks and to their professional success or failure. What follows is a plan for discussing on-the-job employee responsibility for information systems security. In this table, information systems security countermeasures are grouped according to which of three critical characteristics of information they protect: confidentiality, integrity or availability. Furthermore, where possible, each measure can be related to one or more specific ways in which insider or external offenders threaten information. For example, the probability of success by a remote hacker would be minimized by effective access controls. Insider sabotage might be

precluded by effective personnel security and a continuing evaluation program that deals with employee dissatisfaction before it gets out of hand.

Threats and Security Countermeasures for Informations Systems

Critical Characteristics of Information Subject to Threat	Modus Operandi or Criminal Action	Security Countermeasures
1. Confidentiality	Hacking from remote location Unauthorized Access Insider theft of media Illegal sale of data/software Espionage by employee Electronic Eavesdropping Theft of Passwords	Effective access codes Password controls Personnel security measures Security Education Data encryption Multi-level processing Approved systems
2. Integrity	Hacking from remote location Insider sabotage Introduction of virus Alteration/deletion of data	Effective access codes Password controls Personnel security measures Anti-virus software Audit trails Physical security
3. Availability	Introduction of worm to network Insider sabotage Insertion of logic bomb, trojan horse, virus, bacteria	Access controls Anti-virus software Audit trails Personnel security measures

The final message to convey to the audience by the security educator is that good security depends upon everyone's involvement and support in the process and that security professionals are there to help, advise and assist, rather that to apprehend or catch the slacker.

In summary, the probability of success in selling the above four arguments to employee populations will be greatly enhanced by fully integrating security education for information systems into the comprehensive programs for security education. Partitioning out "computer security" as an esoteric specialization automatically creates a barrier to rank and file employee involvement and understanding. Furthermore, much depends upon the educator's ability to accurately define the threat to information systems drawing on current and authoritative counterintelligence reports and up-to-date case information from media reports and other sources. Experience has shown that what our personnel pay attention to

educator's ability to accurately define the threat to information systems drawing on current and authoritative counterintelligence reports and up-to-date case information from media reports and other sources. Experience has shown that what our personnel pay attention to is not abstract generalizations, but real facts about real people and events having consequences or payoffs that everyone can relate to.

References

McCumber, J. R.. *Application of the Comprehensive INFOSEC Model: Mapping the Canadian Criteria for Systems Certification.*

McCumber, J. R.. (1991, September). Security Measures for the State-of-the-Art Workplace. *Security Awareness Bulletin*, pp. 5-9.

Fischer, L. F. (1991, September). The Threat to Automated Data Systems. *Security Awareness Bulletin, 1*, pp. 1-3.

Forche, M. R., & Cutchins, L. E (1993, April 5).. *Computer Crime and Security Incident Study: Michael A. Peri.* Community Research Center, April 5, 1993.

Heuer, R. J. Jr., (1993), April). *Crime and Security Risk: Background Information for Security Personnel.* Monterey, CA: Defense Personnel Security Research Center.

Markoff, J. (1988, November 26). Cyberpunks Seek Thrills in Computerized Mischief. *New York Times.*

National Security Telecommunications and Information Systems Security Committee (1993, August 30). *Incident Response and Vulnerability Reporting for National Security Systems* (NSTISSD No. 503).

Principal Cases of Computer Crime Impacting on Defense-related Information Systems

Name	Date	Systems Penetrated	Damage/Compromise	Stated Motivation
Herbert Zinn (17) (Shadow Hawk)	1987	Bell Laboratories US Missile Command System Robbins Air Force Base	Software theft valued at $1.2 million artificial intelligence advance computer design	-
West German Hackers	1986-1989	Lawrence Berkeley Labs Pentagon systems Los Alamos National Labs NASA	extensive loss of sensitive data	money (KGB operation)
Robert Tappan Morris	late 1988	INTERNET network nationwide affecting Lawrence Livermore Labs, Army Ballistic Research Lab, NASA Ames Research Center	Infected network with virus (worm) shut down network of 6,000 UNIX-based computers	Intellectual challenge out of control
Michael Peri	Feb 1989	(U.S. Army W. Germany)	Passed classified media to East German Intelligence	Frustration at work
Legion of Doom Internet break-in	June 1989	Planted time bombs in AT&T switching computers	Damage at $1 million	Hope of financial gain
Levittown Hacker (15)	Sept. 1989	Grumman VAX system	Military related databases & programs	-
MOD (Masters of Doom) led by Zod (14)	Nov. 1989	Secretary of Air Force	Crashed the system $250,000 to repair Sensitive information compromised	-
Richard George Whitman (24)	March-June 1990	NASA Marshall Space Center Goddard Space Flight Center	Altered/ damaged data	-

Name	Date	Systems Penetrated	Damage/Compromise	Stated Motivation
MOD Mark Abene (20) aka Phiber Optik four other NY youths all 22 or younger)	1990-1992	Southwestern Bell Martin Marietta IT&T; TRW Pacific Telesis Group	$370.00 loss by S.W. Bell, stole passwords, credit information destroyed data	To enhance image, gain prestige, intimidate other hackers
Dutch Teen Hackers	April 1990- May 1991	Kennedy Space Center Pacific Fleet Command Lawrence Livermore Labs Army, Navy, A.F.: 34 sites	Obtained highly sensitive files on U.S. war operations; modified or copied data	-
Australian Hackers Nahshon Even-Chaim (18) Richard Jones (20) David Woodcock (21)	Feb 1990	NASA, Norfolk Lawrence Livermore Labs, US Naval Research Lab. through Internet System	Loss of NASA system for 24 hours; deletions, alteration of data	Boost to self-esteem, fame; enjoyed thrills
Michael Lauffenburger	March 1990	General Dynamics Space Division	Planted Logic Bomb in Atlas Missile parts program	Revenge Lack of recognition
Leonard Rose Jr. (32) (former member of Legion of Doom)	May 1990	AT&T Unix Software	Trojan Horse in software for access to AT&T	-
Levittown Hacker (15)	Sept. 1989	Grumman VAX system	Military related databases & programs	-
Kevin Lee Poulsen (17) (Dark Dante) Ronald Austin (19)	1983-1992	Army MASNET; DoD ARPANET Ft. Bragg; SRI, Rand Corp. Pacific Bell Telephone	Charged with espionage; obtained classified; compromised Federal wire taps	Driven by ego, money, need for recognition
Charles Anderson (19) Costa G. Katsaniotis (21)	Oct 1992	Boeing Aircraft Environmental Protection Agency Goddard Space Flight Center	Illegal access UNIX system, copied passwords	-

Understanding the Computer Criminal

Neil S. Hibler
Director, Community Research Center

and

Jim Christy
Computer Crime/Security Team Chief,
Project Slammer
Director, Computer Crime Investigations
Air Force Office of Special Investigations

Introduction

Among the efforts undertaken by the government to combat computer crime is a scientific study of the criminals involved. The premise of this research is that in order to develop preventive countermeasures and investigative solutions, there needs to be an intimate, insider's understanding of the crime. These efforts approach the problem from the vantage point most intimately aware of all that happened; the perspective of the offenders' themselves. The information sought includes contextual factors, to include the criminal's perceptions and explanations of what, how and why they committed the crime.

This paper introduces a nationally based study that is currently in progress developing new information, specifically seeking to explain intentional violations of computer security systems and the use of computers to commit crimes. The following sections discuss the formation of this research program, the nature of information gathered and concludes with two brief case examples.

Developing a Research Model

Getting one's arms around the larger issue of computer security and crime required a nosology with which to define parameters. That was the first task approached, for once defined, a research design could then address specifics of the larger domain, and able to isolate factors of interest. These issues of interest affected the selection of cases, which is now developing into the database from which all analyses derive.

In order to define "what" to study, a research committee was established, consisting of computer crime investigators from across the agencies of national government. This steering group prioritized their interests by two issues, the mind set of the criminal, and the tradecraft involved.

To consider the criminal mind set, the steering committee formulated a theoretical continuum to describe the *intent* behind subjects' motivation (see figure 1. below)

Figure 1.

MALICE CONTINUUM

BROWSING GAMING CHALLENGING TRESPASSING ALTERING/DESTROYING/STEALING

NO MALICE INTENDED INTENTIONAL MALICE

The clear preference of the steering committee was to establish a research base from cases that involving intentional malice. In so far as tradecraft was concerned, their was interest was to include cases involving current systems that were violated by some representative instances in which common techniques were employed. The driving interest was, however, to study cases involving novel methods and/or applications. Together, these criteria are establishing a data base that is driven by the most malicious cases and newest violations technologies.

This initiative is also a complement to other, on-going efforts that provide anchors for comparison to other security violations issues. The established research model compliments this computer security study by providing a data gathering methodology that has already proven to be successful studying other forms of criminal behavior. Included in the domains of information gathered by the common structured interview protocol are details regarding the subject's life span, as partitioned by relationships, family issues, education, employment, and medical condition. One section of this inquiry details the criminal behavior, it's causes and the efforts conducted to bring it about. Further collaborative information is obtained from those who knew the subject at the time the crime was being committed. These sources include work place associates (i.e., coworkers, supervisors) as well as intimates (spouse, girlfriends, boyfriends, co-conspirators, etc.). As additional informants, they provide confirmation of subject's statements, and add their own insights as to influences on the criminal behavior.

The remaining source of personal information is psychological testing. Standardized examination instruments are used to measure intellectual functioning and personality characteristics, to include self-esteem, social skill, and mental status. Interestingly, early attempts to measure personality features were feared to be superficial, because often there were considerable intervals between the law-breaking behavior and testing. What the earlier research has shown is that those underlying personality traits that show risk, do not

change over time. Further, these features have demonstrated considerable differences from persons who do not commit crime. The remaining area of interest, is exactly how these subjects committed their crimes.

The structured interview includes a section that explores the criminal acts and influences on them (this section is included in the Appendix). Of course, both barriers and impediments to the crime are of interest; the protocol is the stepping off point to as full an complete an understanding as is possible. In order to facilitate the capture of all that subjects say, the entire interview is video taped. This "modern" aid to recording is helpful making records that are easy to review, and are further contributed to by yet other record making devices.

Capitalizing on advances in simulation technology, researchers include an environmental test bed component. A state of the art main frame computer has been partitioned, so that with an extensive library of software, it has been possible to create configurations that duplicate virtually any data system. The resulting conditions are accessible by modem, permitting researchers to give subjects a modem linked notebook computer and ask them to recreate their crime. As the (simulated) information system is accessed, subjects' every key stroke is automatically recorded.

In total, this research effort is a collaboration between a variety of disciplines, each working closely with the other to build a better understanding of computer crime, and how to prevent and investigate it. Cases studied to date have provided many interesting details. The brief summaries that follow provide a look at some of the information that is developing.[1]

Case Examples

Case 1.

An example of low tech computer crime, this case began when a U.S. soldier decided to abandon his duty station and to defect to a foreign nation. Incidental to this plan, the soldier brought with him a standard lap top computer, and two floppy disks that contained sensitive information. The disks were to provide a sense of bona fides, as well as a (hoped for) sense of recognition and advantage.

The soldier was surrounded by various stresses. Included were persons with whom he could not get along, peers and supervisors who were critical of his work. Just the same, he had a clean record, so much so that he was to be interviewed for recognition as "Soldier of the Month." Just the same, he had great difficulty in making effective interpersonal

---

[1]These summaries are based on a series of case reports, "Computer crime and security incident study," authored by Michael Forche, the Community Research Center.

relationships. He had no real anchors to rely on, no one with whom to seek solace, nor to air his frustration. His defection was an act of desperation.

This subject's knowledge of computers was so primitive that he didn't know how to copy disks, or even how to list files. He brought along the laptop computer because he didn't know if the service to which he would defect had a means to read the classified disks. He had no idea that the computer's hard drive had once held documents even more sensitive than those he stole. Unfortunately, the opposition realized what had been handed to them, they had no difficulty in recovering everything that was of value. In a surprising twist of fate, this soldier was tried, convicted and sentenced. In jail, he was assigned to duties in the prison library where he learned to use an MS DOS system for tracking the library's holdings. He told researchers that if he knew then (about computers) what he knew now, he could have created damage of many times the significance of his already terrible destruction. Fortunately, this subject was naive regarding computers. This is very different from other cases in which the criminal had advanced knowledge, and every intent to use it exploitively.

Case 2.

This is the story of a youthful offender who was able to conduct sophisticated violations, resulting in several hundreds of thousands of dollars. Beginning at thirteen years of age, he committed over two thousand computer crimes, and was arrested and convicted of only one. He admitted to using computers to gain unauthorized entry into commercial telephone computer systems to find access codes and numbers. He admitted using phreaking activities to eliminate long distance phone charges by using an unauthorized voice-mail system, 1-800 numbers, and customer's access card numbers. His illegal activity included obtaining copies of credit reports and credit card numbers. This perhaps, is the foreshadowing of things to come.

The subject is a hacker who explores the cyberspace networks of computers in order to communicate with other hackers. At the time of his arrest, he appeared to be an "All-American" kid. He was a high school honor student who had been awarded a full college scholarship. He worked after school, using the income to finance his computer hobby. He was described as coming from a stable home, with only minor trouble preceding his arrest. Friends considered him to be an introverted person, nearly absent in interpersonal skills.

The major reasons for this subject's illegal activity included curiosity and intellectual challenge. Hacking provided the opportunity to expand his horizons, he used bulletin boards to relate to other hackers and to explore far away places. Interestingly, his local co-conspirators were also superior students, and each had a history of learning disabilities in elementary school.

CASE 3.

This was a co-conspirator of the subject in case 2., he was also a teenager (age 16), but unlike the "honor student" profile of the preceding case, he was cocky and abrasive. Others, particularly adults, found him to be a liar who enjoyed game playing with superiors; wholly untrustworthy. He was physically small and self-conscious, but hid it with his "in your face" attitude. His parents were separated, his father was being treated for depression. The family tree was also fruitful. A grandfather had died in prison, he was a felon, twice convicted for armed robbery.

In so far as hacking was concerned, this subject found particular pleasure in looking at people's records, he enjoyed violating their privacy. In some instances, he wanted to cause them trouble, he would obtain credit reports, but did most of his mischief by running up telephone bills. His utmost fantasy was to enter into a computer system in which he would have the power to launch a space shuttle or to start a world war. He was so consumed by his hacking, that he thought it better than sex.

The vindictive side of this subject was almost limitless. He was proud that he was able to be disruptive. Among the intrusions he was responsible for were cancellations of garbage and water services, passing along telephone numbers of those targeted to other hackers (by placing them on a hacker bulletin board), and interrupting operating systems by removing entry access to authorized users. All of this nefarious activity was experienced without regret. To quote the subject, "If I abuse the PBX, AT&T benefits ... the private owner still has to pay ... AT&T gets a lot of their profit through hackers because they call illegally and make other people pay for it."

He was no stranger to the police. There had been a fight in elementary school which had to be settled by the authorities and later, when he was 14, he was arrested for stealing a car phone. A year later, his parents were contacted by the police because he was hacking into a commercial voice mail system. Security personnel from the telephone company had also reached the mother, but all she ever did was yell at him.

Perhaps among the most interesting findings from this case was the generalizability of the motive to many other hacker cases. This computer criminal did not start out to be a criminal at all. His introduction to the world of hacking was simply to accommodate computer activities which used telephone lines, and were therefore unaffordable. His use of the computer world to annoy others developed only later. He estimated that he committed over one hundred ccomputer assisted offenses, but was caught and punished for only one.

CASE 4.

Like the two previous teenagers, this subject suffered from learning disabilities while a child. He had been diagnosed as having Attention Deficit Disorder and for most of his elementary school years was medicated with Ritalin. In high school his behavior problems changed in form, from being learning inhibiting to being socially unacceptable. Despite better grades in high school, by the time this subject was seventeen he was using marijuana four times a week, and taking one to four doses of LSD one day a week. In fact, he often used drugs while hacking.

He was unreliable, but didn't see it. For instance, he had been fired from a job at a service station for suspicion of theft. He seemed to fuss about the accusation, even though he admitted to researchers that he had been skimming proceeds. He had also been arrested. Shortly before he was detained for hacking he had broken into two automobiles. His intent had been to steal something he could use to pay his rent. He plead guilty to two counts of burglary, two conveyance and two for petty theft. He was on two years probation (a plea bargain) when he was investigated for his computer crimes.

He claims he had been hacking for only nine months, his motive was ostensibly to seek out opportunities for profit, but ego needs seemed to be the force behind it all. "I felt that at some point I was going to discover something to make me wealthy, powerful or both, whether it was fraud opportunities or recruitment by foreign or domestic power for somebody of my talents." His own attempts were initially fruitless, but he was able to hook up with a mentor (a twenty-four year old) who taught him how to penetrate systems. Interestingly, this mentor gained much of his knowledge on system vulnerabilities by keeping up to date on government published computer security advisories.

Conclusions

As these very brief case discussions suggest, there is a great deal to be learned about computer crime by studying computer criminals. It does not appear that effective countermeasures or truly effective investigative procedures will be possible until there is a more complete understanding of this crime, and in particular, influences on the commission or cessation of wrong doing. The research described in this paper is yet new, it is hoped to develop information that will identify patterns of behavior from which crime fighting advances can develop. To do that, the Federal government is relying on insights from the criminals themselves; it's a process that has proven to be helpful in other types of criminal activity. There is also much to learn from each other. Yet methods of computer crime prevention, detection, and investigation should be shared among law enforcement professionals in ways that protect any advantages that research may provide. We need to be consumers of our own findings, especially those that preserve the security of our own crime fighting efforts.

Notes on Peopleware: Downsizing, Resentment, Sabotage and Espionage[2]

Theodore R. Sarbin
Defense Personnel Security Research Center

We are living in an age of expanding violence. I want to suggest that sabotage via malicious intrusions into computer networks is a form of attenuated violence. As I suggest later, the destruction of information stored in computers may become the choice of disgruntled employees. Traditionally, terrorists resort to physical violence, but it is not difficult to imagine their engaging in computer sabotage. I will come back to the topic of sabotage, but first some preliminary remarks.

One of the main reasons for the existence of security organizations is to prevent the betrayal of trust, more specifically, the disclosure of secrets entrusted to certain persons and not others. We design employment procedures with the intent of screening out untrustworthy people. Our indoctrinations are designed to inform cleared employees how to go about the task of keeping the secrets. Notwithstanding our best efforts, an unknown number of presumably trustworthy people betray the trust. Identifying the parameters of trust and betrayal is central to many of PERSEREC's research programs.

The trust-betrayal theme takes on additional importance under the current downsizing in industry, government, and the military. Many employees will lose their jobs. We can assume that most of these employees will find ways of adapting to the event as a contingency of life. Some unknown proportion will interpret their dismissal differently. If they have built their life stories around the notion of a continuing career, they may perceive themselves as victims of unjust authority.

It is instructive to make use of a concept that is the centerpiece of studies in personality: the concept of identity. Briefly, this concept is the composite of answers that a person constructs to the ever-recurring question: who am I? For many persons, the central feature of one's identity is his or her career. Such an employee may well interpret the layoff or discharge as an assault on his or her identity, and further, lead the employee to identify himself or herself as a victim of unjust authority. The self identification as victim carries with it the notion of powerlessness. In this narrative, anger and resentment become the guides for action. The self-as-victim story implies the existence of a victimizer. The initial response for victims of unjust authority is to entertain the idea of retaliation against the perceived or imagined victimizer. In the victims' imaginings about retaliation, who would be the likely target? Available to be cast in the role of victimizer are a number of familiar abstract entities: the corporation, the government, the Pentagon, the bureaucracy.

---

[2]An earlier version of this paper was presented to the Department of Defense Security Institute conference in 1992.

To be sure, not all victims of unjust authority engage in retaliatory acts. It is one thing to entertain the idea of getting even, it is another to perform acts of sabotage or espionage. Such deterrence factors as risk-assessment, the imagined experience of shame if discovered, and the strength of one's conscience could derail an imagined retaliatory scheme.

In the history of industrial society, the resentment narrative has been the motive force for sabotage. The early 19th century Luddites, displaced by wool fabricating machines, perceived themselves as the victims of injustice and attacked the machines that they construed as the cause of their victimization. The pattern of the Luddites has not been lost on contemporary workers, e. g., a disgruntled employee intentionally "forgets" to follow safety procedures resulting in damage to machines and a slowdown in production.

We are familiar with the more common forms of sabotage: destruction of equipment or supplies, stopping or slowing necessary activities, theft and pilfering of tools and work products, goldbricking, absenteeism, false fire alarms, and bomb threats. Not usually construed as sabotage, the theft and mismanagement of information stored in computers may be added to the list of acts directed toward achieving retaliation.

Acts of sabotage are aimed at satisfying two kinds of objectives: instrumental and demonstrative. In instrumental sabotage the employee has a specific goal and he or she stands to gain something, e. g., payment from a person interested in destroying expensive equipment. In demonstrative sabotage, the saboteur's goal is to embarrass the entity that he or she perceives as the victimizer. His or her sabotage efforts are clandestine forms of protest against perceived or imagined injustice or injury. Because the individual is usually powerless to change a management decision, he or she may attempt to nullify the negative identity of being a victim through strategies of empowerment. Sabotaging a computer network, for example, would be a demonstration that the saboteur was able to dissolve the unwanted victim identity and replace it with a more acceptable identity based on power and competence.

The sabotage metaphor is especially applicable to understanding some aspects of information security, especially the unlawful use of computers. Instrumental sabotage would be exemplified in the retrieval and marketing of government or trade secrets by persons who have authorized access to relevant computers. Demonstrative sabotage would be exemplified in the acts of computer users who introduce viruses, logic bombs, and other malicious features the intent of which is to create chaos.

Traditionally, information security specialists have been concerned with unauthorized disclosures, especially espionage. The premise for the security specialist and for the potential offender is that government and trade secrets have value. Having value, secret information may be conceptualized as a commodity, a product that can be bought and sold.

From multiple sources--television news, the press, historical accounts, biographies, and spy novels--all of us have been made aware that an information market exists. For many years, the information market was dominated by Soviet bloc countries. Technological and strategic information was sought and sometimes delivered by American citizens who had been cleared as trustworthy stewards of some of the nation's secrets. In a competitive technological world, information markets will continue to flourish. The buyers may speak with accents different from the Cold War stereotypes but we can assume that they are ready to exchange cold cash for warm secrets.

As security specialists, we have learned a great deal about citizen spies and have concluded that the real or imagined need for money is the primary force behind their crimes. To be sure, the money served as the medium for satisfying other needs, such as power, vanity, status, protection. We have heretofore been less concerned with resentment as a motive even though it is a significant feature in some cases. In the 1990s, security specialists must be sensitized to the potential for resentment. Generalizing from studies of unemployment, the frequency of resentment is likely to reach a new high under the downsizing policies.

Let us consider the phenomenon of instrumental sabotage as a strategy of retaliation for perceived victimization. Employees with security clearances have a special retaliatory tool--they have access to secret or sensitive information. As I mentioned before, converting secrets into marketable commodities is one form of retaliation. Successfully executed espionage provides the offender with personal gain, at the same time "getting even" for an assault on his or her identity.

PERSEREC studies have concluded that citizen espionage and embezzlement are exemplars of a general model the center of which is the granting and betrayal of trust. Given this construction, the control of computer crime calls for at least three interrelated approaches: (1) the continuance of efforts to develop information and physical security safeguards in computer technology to discourage and derail both types of information sabotage; (2) better selection of personnel for positions of trust; and (3) deterrence. I forego a discussion of the first approach, first because PERSEREC has no in-house competence in computer technology and does not pretend to offer suggestions on encryption, passwords, etc., and second, computer security technology is a fast-growing industry. The second approach, selecting trustworthy personnel, is within the competence and interest of PERSEREC staff members. (In this connection, PERSEREC has a large scale project under way the potential results of which will identify persons at high risk for trust betrayal, the necessary antecedent both to instrumental sabotage and demonstrative sabotage.) Ultimately, the findings of the study will contribute to an understanding of the contributions of psychological characteristics to the enactment of the two types of sabotage: (1) the identification of persons who would be at risk for participating in the illegal, if not treasonous, information market, and (2) the identification of persons who

would be at risk for using their access to computer networks to create chaos, such as spreading viruses, malicious intrusions, and other criminal acts.

In another place in this report, Dr. Sherizen has given us an overview of deterrence from the criminological perspective. Rhonda MacLean has demonstrated that an effective deterrence program must be more than a casual briefing on security awareness. In the present context, employees whose performance on an assessment battery would classify them as high risk personnel would be persons who were ready to perceive themselves as victims of an uncaring corporation or bureaucracy. However, before placing complete reliance on psychological assessment, a cautionary note is in order. Like all assessment instruments, a degree of error is to be expected. False positives and false negatives are inevitable. If we assign trust to an employee on the basis of background investigations or psychological assessments and he or she violates the trust, we look for reasons for the faulty prediction. When we engage in such an examination, we are reminded that conduct, whether moral or immoral, lawful or unlawful, is not exclusively determined by self-characteristics. The use of psychological inventories and background investigations reflects an orientation in which background factors revealed in the investigation are assumed to have causal status. An alternate and complementary orientation focuses on the foreground of criminal acts, the constellation of personal, organizational, and societal conditions present at the time the offender plans and executes a criminal act. To assess foreground factors, we examine as much of the total context as we can. In the foreground, for example, would be the announcement that one's career is being aborted, a condition, as I suggested before, that would influence the construction of a victim-victimizer scenario.

Two aspects of the context can be identified: personal and organizational. The following questions guide an examination of the personal aspects of the context. Answers to these questions would illuminate the personal conditions in which temptation to crime takes place. What is going on in the life of the employee? Has he or she had financial reverses? Has the employee been getting along with fellow employees and supervisors? Has an effort been made to convince the employee of the rationality and necessity of management's adverse personnel decisions? In addition to asking questions pertaining to the personal aspect of the total context, we can ask questions pertinent to the organizational context: What is the social climate of the organization? What are the prevailing attitudes toward information security procedures? Is there an effective deterrence program? Does management promote attitudes that neutralize the cynicism often expressed about information security? Do the employees express commitment to the goals of the organization? Or, conversely, does the organizational climate foster alienation?

In brief, we need to augment the assessment of life style with continuing assessments of personal and organizational contexts in order to understand the reasons a trusted person,

under conditions that foster resentment, would entertain a plan to commit an unlawful retaliatory act.

The problem confronting us can be stated concisely: What can be done to neutralize the effects of being fired so that employees with security clearances will not betray the trust by disclosing government or trade secrets or by engaging in other forms of sabotage?

The best countermeasure to resentment is to reconstruct the scenario to attenuate the victim-victimizer construction. In psychological terms, the most effective countermeasures would communicate to the employee the notion of care. It is important to stress that care is a sentiment that cannot be attributed to an abstract entity such as a bureaucracy or a corporation. Care is mediated by persons. It is the sentiment that bonds friendships, parent-child relations, and primary groups. In the victim-victimizer scenario, the personnel who mediate between the victim and the faceless government or remote corporation are not necessarily identified with the abstract victimizer. Persons with proper names--supervisors, officers, chaplains, ombudsmen--are not likely to be perceived as the source of the employee's perceived victimization. These men and women can serve as agents of care. In face-to-face relations, the supervisor or officer can neutralize the victim-victimizer scenario and replace it with an alternate scenario that centers on the phenomenon of care. The details of the communication will vary with conditions. The officer should avoid the traditional one-time exit interview that could be perceived by the terminated employee as similar to a clergyman delivering the last rites to a dying patient. Some suggestions for the content of interviews would include: the supervisor provides detailed explanations and justifications for the dismissal (to offset the impersonal effects of the traditional pink slip); the supervisor offers to help the employee find alternate employment; the supervisor indicates a readiness to give advice on retraining and other options; the supervisor makes referrals to appropriate helping agencies; in an important way, the supervisor continues as the agent of care with follow-up phone calls and/or letters. Clearly, these suggestions do not exhaust the possibilities.

To sum up: the problem of resentment is a critical one for information and personnel security, given the number of personnel with security clearances who, in the next few years, will be laid off, fired, or asked to retire. An unknown number will interpret the action as victimization and will harbor resentment. Relying on the sabotage metaphor, I have argued that some employees will engage in acts of trust betrayal in order to retaliate against the government or the corporation. Because nearly all information is stored in computers, the betrayal of trust involving government or trade secrets is simultaneously a problem for both information security and personnel security specialists. One implication of this analysis is that the problems identified are multiple and that their resolution calls for collaborative study and research by specialists of different skills and interests, such as those who have participated in this conference.